Anno 1 - N. 13
21 novembre/5 Dicembre 2002

Boss: theguilty@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Graphic designer: Karin Harrop

Contributors: Bismark.it, Tuono Blu, CAT4R4TTA, lupinIII, Enzo Borri

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00187 Roma - Piazza Colonna, 361-
Tel. 06.69514.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

Realizzato con la collaborazione di Hacker News Magazine - Groupe Hagal Arian

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hăk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

VOLEVATE UN CD? E NOI VI DIAMO ANCHE UNA SECONDA RIVISTA!

Prendendo a caso una manciata di messaggi ricevuti dalla redazione, ne troverete tre che chiedono di allegare un CD-ROM alla rivista, altrettanti che ci invitano a non farlo per non incidere sul prezzo, un paio che vogliono articoli più tecnici, qualcuna che chiede tutorial e guide per i programmi più utili, mentre altri preferiscono trovare queste informazioni in rete, e da HJ vogliono più notizie, più attualità e qualche riflessione sulla filosofia dell'-hacking.
Finora abbiamo fatto quello che potevamo per cercare di accontentare un po' tutti, cercando di mantenere quel delicato equilibrio che è alla base della alchimia "Hacker Journal". Quello che non abbiamo mai potuto fare è aggiungere "un po' di CD-ROM".
Ora, se qualcuno ha avuto il dubbio che fossimo pazzi quando abbiamo deciso di far uscire Hacker Journal, ora il dubbio se lo toglierà del tutto: oltre ad Hacker Journal, ora tiriamo fuori dal cappello un'altra rivista, Hackers Magazine, con CD-ROM allegato.
Così chi vuole a tutti i costi un CD lo avrà, e chi preferisce avere HJ a 2 euro, potrà continuare a farlo senza timore di aumenti di prezzo.
Oltre alla presenza del CD allegato, Hackers Magazine da molto più spazio ai tutorial, grazie a guide passo a passo che spiegano dettagliatamente come utilizzare i programmi che si trovano appunto sul CD-ROM. La trovate già in edicola, al prezzo di 4,99 €, e ce la troverete tutti i mesi (Hacker Journal continuerà invece a uscire ogni 14 giorni, il giovedì).
Detto questo, vogliamo precisare una cosa: nonostante la "parentela", le redazioni delle due riviste sono in realtà separate. Evitate quindi di mandare a una le richieste o i commenti relativi all'altra.
Buona lettura...

grand@hackerjournal.it

La cosa giusta

Volevo rispondere in due righe agli articoli apparsi nelle pagine di Hacker Journal, visto che in quanto hacker vecchia scuola non mi ritrovo nelle opinioni di Genocid3 autore dell'articolo a pag. 3.

Intanto una precisazione storica: l'hacking nasce negli anni 50 al MIT sui PDP, anche se già da prima alcuni gettavano le basi sugli IBM 370, che non ha avuto successo perché macchina batch gestita da operatori capoccioni... questo spiega anche la tendenza alla libertà individuale dell'hacker, che NON è anarchia, come molti ritengono, semplicemente **un hacker non tollera che ci siano imperfezioni in un sistema (qualunque esso sia)** e da questo scaturisce il suo odio verso chi gli impedisce di fare 'la cosa giusta' (ovvero migliorare il sistema)
Confondere questo concetto di libertà di operare per migliorare il mondo in cui esistiamo con l'anarchia è l'errore che ha portato alla diffamazione del genere 'hacker', personaggio oggi visto come un pericoloso criminale.

Inoltre **c'è un motivo per cui gli hacker diffamano windows... è NON è filosofico ma pratico**. Ma prima una piccola premessa: a tutt'oggi windows è la MIGLIORE piattaforma per videogiochi esistente, e con questo so di attirarmi addosso l'ira dei programmatori di winex. Comunque per adesso le cose stanno così, non esistono concorrenti diretti.

Il motivo per cui quando programmo, lavoro o tratto dati sensibili in generale uso preferenzialmente un sistema *NIX è perché questi sono molto più flessibili. Non limitiamoci a vedere solo le applicazioni di word processing, che comunque hanno raggiunto un discreto stato di maturità sotto gli *NIX e poco hanno da invidiare ai prodotti commerciali, ma vediamone anche la facilità di programmazione, resa possibile dalla stabilità del kernel, le API ben documentate, grazie allo sviluppo open source, o anche solo la sicurezza di un journaled file system.

Semplicemente windows NON è la cosa giusta. Non siete stufi di vedere ore di lavoro perché word/explorer/lotus/altri si piantano, mandando in crash anche il Kernel (che dovrebbe essere al sicuro due strati di syscall più sopra)? E **la soluzione non è portare l'open source sotto windows** (dispendioso/lungo/inefficente vedi OpenOffice). **La cosa giusta c'è già, è lì gratis alla portata di tutti, sono i sistemi open source**.

Questo manda in bestia noi hacker della vecchia scuola: non solo un sistema altamente inefficiente perdura, ma gode di sostenitori di spicco (aziende/politici/utenti) che lo difendono! Non siamo contro windows, ma se ci sono modi migliori per ottenere un risultato sosteniamo (è qui provate a contraddirmi) che siano questi a dover essere usati.

Ai newbie, a chi si volesse semplicemente documentare o a chi vuole arricchire la propria cultura consiglio Hackers!, di Steven Levi

RAD
nonsaichisono@libero.it

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

NEWBIE

MID HACKING

HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

mailto:
redazione@hackerjournal.it

ACQUA E CRISTALLO...

Salve ragazzi, vi faccio i complimenti per la rivista, che seguo dal primo numero e sta diventando sempre + interessante mese dopo mese. Io + che con la programmazione mi diletto con lo spippolamento hardware e vorrei mostrarvi il mio PC, dopo che ci ho messo le mani sopra.
Le foto si trovano all'indirizzo http://modding.pctuner.net/VostriLavori/Case%20Mugan/Mugan%201.htm Beh, che so... sarebbe una figata immensa vedere un foto (anche piccina :)) sulla rivista, sarei il ragazzo + felice della terra ! Vabbe dai, lo so che esula dal contesto, vi saluto, e continuate così!!!

MuGaN

Eccoti accontentato. Il case è decisamente bello, e il raffreddamento ad acqua una finezza tecnica non da poco.

PROBLEMI TENNICI

Da quando ho installato PincoPallino soft, quando cerco di avviare Explorer mi parte Quake 3, ma quando provo a cambiare arma il lettore di CD spara fuori il disco e mi da il messaggio "Errore di sistema incomprensibile". Secondo voi dovrei passare a Linux?

Lettore disperato

OK, la domanda è inventata di sana pianta, ma vi possiamo assicurare che di richieste simili ne arrivano proprio tante. Il tutto è una scusa per dire che purtroppo non possiamo risolvere personalmente i problemi di tutti i lettori. Non per questo dovete sentirvi soli. Potete infatti chiedere aiuto agli altri membri della comunità di Hacker Journal, attraverso il forum del sito oppure sul canale irc #hackerjournal, su irc.azzurra.org. Potreste trovare persone disponibili a darvi una mano (ma chiedete con gentilezza e non date per scontato che tutti siano lì per risolvere i vostri problemi).

PROGRAMMI IN ITALIANO

Ho appena comprato il N° 12 di hacker journal, sfogliandola, mi sono imbattuto su una lettera di un vostro lettore che chiedeva se il programma Zone Alarm fosse disponibile anche in italiano, e voi avete detto di no. Invece non è così: esiste una patch che traduce dall'inglese all'italiano, e si trova su http://tradusoft.supereva.it, dove sono presenti moltissime traduzioni per svariati programmi. Potreste anche pubblicare il link del mio sito: www.stefloyd.it?

Stefloyd

Pubblico la segnalazione, ricordando però che se si vuole patchare un programma conviene farlo scaricando file solo da siti affidabili. In una sedicente "traduzione" potrebbe anche nascondersi un virus o un trojan.

RISPOSTA A MODEM LENTO

Spero di essere d'aiuto alla comunità. La lettera di Niger di qualche numero fa ha richiamato la mia attenzione, forse perché ho già ho dovuto affrontare il problema in passato. Non ho capito la piattaforma su cui si voleva ottimizzare la connessione. Io vi descrivo la soluzione attuabile su piattaforma Win9x, da provare su Win2K ed eventualmente su XP:
1.. connettersi ad internet, con l'account da ottimizzare (non avviate ne IE/NS e Outlook/Eudora ed affini)
2.. Da Start - Esegui - immettere il comando WINIPCFG - dalla finestra "Informazioni sulla scheda" appuntarsi l'indirizzo IP (attribuito dinamicamente dal provider con cui è attiva la comunicazione) es. 10.123.158.78 ;
3.. Aprire una sessione di Ms-Dos e digitare il comando ping -f -l 500 10.123.158.78 - Attenzione: dovete mettere l'indirizzo rilevato da voi sulla vostra connessione; con questo commando apparirà un messaggio del tipo "trasmessi 4 ricevuti 0 persi 4" (100% persi). Il parametro "500"(x) specifica la dimensione dei pacchetti selezionati ed è quello che dovete ritoccare poco a poco (50 byte alla volta, ad. esempio) fi-

Doverose scuse

Un lettore ci ha segnalato che l'articolo su Ping e Traceroute pubblicato sul numero scorso a firma di Matrox, è stato in realtà copiato da un vecchio documento realizzato dagli Spippolatori (www.spippolatori.com). Inutile dire che i primi a essere stati presi in giro siamo noi, e che non rivedrete mai più quel nome sulla rivista, ma vogliamo ugualmente scusarci coi lettori e con i veri autori del testo.

Saremo di nuovo in edicola Giovedì 5 Dicembre!

STAMPA LIBERA NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

no a raggiungere il valore appropriato/ottimale per la connessione VOI -> VOSTRO PROVIDER; come capirlo: semplice, dopo continui ping -f -l x 10.123.158.78 fermatevi quanto ottenete il messaggio "trasmessi 4 ricevuti 4 persi 0 (0% persi) io ho ottenuto un valore pari a 248 byte;

4.. Chiudere la connessione ad internet;

5.. Da Start - Esegui - immettere il comando REGEDIT (attenzione siete nel registro di configurazione di Windows, se non siete pratici lasciate perdere, se amate il rischio: auguri);

6.. Individuate la chiave HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\Net\0000\Ndi\params\IPMTU\enum Se non vi siete ancora persi e tenendo aperta questa chiave, selezioniamo dal menù Modifica le opzioni Nuovo e Valore di stringa, ora digitate qui il valore ottimale della vostra connessione, quello appena trovato. Ora entriamo nuovamente nel menu Modifica scegliamo l'opzione Modifica e digitiamo un nome identificativo ad. es. concenti. Chiudere il registro di Windows.

7.. Riavviare il computer;

8.. Riavviato accediamo ne menù Start - impostazioni - Pannello di controllo, RETE , Dispositivo di accesso remoto , Proprietà Avanzate, selezionare ora la voce "Dimensione del pacchetto IP" e nella parte destra scegliere la nostra dimensione ottimale battezzata prima come Connect.

9.. Riavviare il computer

10.. Ora sarete regolati al massimo con la banda concessa dal vostro provider internet, l'aumento di velocità sarà + o - apprezzabile.

ANTOEDP

Di solito, questo tipo di modifica produce risultati migliori con collegamenti a larga banda, ma tentar non nuoce (sempre e comunque avendo fatto un backup del Registro prima di metterci le mani...)

PASSWORD DI UN DOC

Ho perso la password di un file .doc (Microsoft word) che voi sappiate c'è il sistema per scavalcare questo inconveniente?

Alle

Arrivi a tutto quello che esiste (o quasi) a partire dall'indirizzo: http://directory.google.com/Top/Computers/Security/Products_and_Tools/Password_Recovery/

ABBONATO SVANTAGGIATO

Facciamo un discorso tra brave persone sul prezzo dell'abbonamento ad HJ da voi fissato. Il prezzo che avete pubblicato sul n° 12 di HJ è di Euro 49.90 25 numeri + un cappellino di HJ che ad acquistarli in edicola verrebbe a costare Euro 50.00 senza il cappellino. Ok qui tutto va bene ad eccezione di una cosa: possiamo pagare l'abbonamento solo tramite c/c postale e ciò comporta una tassa di Euro 0.77 quindi tutti sanno effettuare una somma tra due numeri: 49.90+0.77=50.67. Dunque verrebbe a costare Euro 0.67 in più in confronto ad un acquisto di 25 numeri in edicola.

[J]ump[y]

Sai qual è il problema? È che HJ costa troppo poco. Il costo della spedizione incide così tanto che se facciamo prezzi più bassi, ci smeniamo (anche perché la gestione dell'abbonamento ha un costo fisso, oltre alla spedizione di ogni singola copia, e se non raggiungiamo un certo numero di abbonati rischiamo grosso). Ovvio che avremmo voluto proporre un abbonamento con uno sconto molto succulento, ma avremmo finito col rimetterci pesantemente. Per ora di meglio non possiamo proprio fare, purtroppo.

LA CLASSE NON È ACQUA

Alla Smau quando ci avete (dopo innumerevoli preghiere) dato quell'ultimo poster rimastovi vi avevamo promesso una foto della nostra classe dove -ovviamente- avremmo affisso l'enorme manifesto. Le reazioni dei docenti sono state piuttosto vivaci ma sono state prontamente messe a tacere dai nostri fidati M-16. Orbene

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: 8ni
pass: ro20

adesso non cercate di fare la stessa fine e PUBBLICATE QUESTA FOTO! Riccardo, l'eccezione che conferma la regola.

Wow. Che onore. Però armi&fucili di 'sto periodo è meglio lasciarli da parte...

CORSO DI C A PADOVA

Sono una vostra lettrice di Padova e vorrei lanciare un annuncio dal vostro giornale. Sto cercando un corso di linguaggio C. Purtroppo non riesco a trovare nessuno: chi sa indicarmi qualche corso valido?

Liliana

Appello prontamente lanciato. C'è qualcuno in zona che conosce validi corsi di formazione?

PRECISAZIONI SU IRC

Salve Hj! Vi scrivo per farvi un paio di correzioni sull'articolo da voi pubblicato sul numero 11, riguardante l'ircwar. Vorrei chiarire due punti, il primo con la speranza di incuriosire qualche lamerazzo che, capendo come funziona il programmino col quale si diverte a "buttar giù" gli utenti delle chat, magari avrà voglia di saperne di più e si indirizzerà (spero) sulla strada del vero hacking; la seconda precisazione la faccio con l'intenzione di scoraggiare il lettore lamerazzo, perché in realtà la cosa non e' così semplice come voi l'avete fatta sembrare. Punto primo: l'attacco nuke.
Non è assolutamente vero che un attacco nuke e' simile ad un attacco flood, e non e' vero neppure che (cito) "il nuke ha come principio l'invio massiccio di dati da un PC. Un attacco flood agisce "sovraccaricando" la connessione, un attacco nuke agisce CREANDO ERRORI NELLA connessione. Un programma nuke, invia stringhe non riconosciute al BIOS, messaggi qualsiasi, una qualsiasi sequenza di caratteri che non essendo riconosciuti dal BIOS, ne provocano il congelamento; un altro tipo di nuke invece sfrutta bug del client sempre inviando stringhe "velenose" (nuke in inglese vuol dire per l'appunto veleno). Anche il D.o.S in un certo senso può essere considerato un nuke. Punto secondo: lo split. Avete scritto "pochi utenti sono in grado di causarne uno, ma tutti possono utilizzarli quando presenti". Attenzione, non e' così semplice, questo era vero solo fino a qualche anno fa. I server di IRCnet usano protezioni apposite per nick e canali in caso di split rendendo indisponibili nick già usati prima dello split o canali già joinati per 15 minuti (ma spesso anche di piu'). Ma dico, avete mai visto uno split "naturale" durare più di 15 minuti?? Per quanto alto, il LAG (tempo di latenza) che causa lo split di un server, non sarà mai abbastanza alto da far durare lo split piu' di 15 minuti. Quindi l'unica soluzione per il taker è causare egli stesso lo split, tenendo sotto smurf un server per molto, moolto tempo. Solo così sara' possibile ciclare il canale da takkare per prendere l'op, o usare i nick dei bot da far killare. Quindi i poveri (?) lamerazzi non hanno vita così facile come puo' sembrare. Cari taker, se siete abbastanza in gamba da smurfare (sempre che sappiate cosa significa e non usiate programmi automatici che non sapete manco cosa fanno), perché non impiegate il vostro

Saremo di nuovo in edicola Giovedì 5 Dicembre!

STAMPA LIBERA NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

tempo in cose più utili invece di perderlo rubando i canali altrui?

D4rkDru|D

FTP E LOGO DI WINDOWS

Nel numero 12 a pag. 28 nella sezione programmazione (ECCEZIONALE!!!!) spiegate come sia possibile connettersi al servizio FTP fornito dal mio ISP. Io ho provato a scrivere "telnet ftp.libero.it 21", e arrivo a definire l'user e la pass, ma continua a rispondere "530 Login incorrect". Dov'è che sbaglio? Per collegarmi a libero scrivo come user mio_nomeutente@libero.it e come password mia_password: sono gli stessi che devo inserire nel collegamento telnet o sbaglio? Come si fa a sostituire in Win98 l'immagine di avvio di win? (Nel 95 c'era un file logo.sys, ma nel 98 nn lo trovo!) Grazie e continuate così.
Distinti Saluti.

Occhio. Non è detto che il tuo provider offra questo tipo di servizio. E in effetti Libero non consente un accesso riservato ad aree riservate del server ftp, ma solo l'accesso come utente anonimo (username: anonymous, password: tuoindirizzoemail). Gli accessi ftp riservati solitamente si usano per aggiornare un tuo sito Web; se hai un sito su Digiland, per esempio, avrai un accesso con nome utente e password a ftp.digiland.it Per quanto riguarda l'immagine di avvio in Windows 98, devi creare una immagine in formato bitmap (BMP) di 320X400, a 256 colori e salvarla col nome LOGO.SYS dentro c:\. Poi devi inserire la riga

LOGO=1

nel file nascosto MSDOS.SYS, alla riga [OPTION].

IL NUOVO SITO DI HACKER JOURNAL

Newsletter
Inserendo qui il tuo indirizzo email, rimarrai informato su tutte le novità che riguardano la rivista: gli argomenti dei nuovi numeri, i servizi per i lettori, le nuove offerte.

Email gratis!
Da qui puoi accedere alla tua casella di posta con indirizzo @hackerjournal.it, o registrarne gratuitamente una, se già non ce l'hai.

SecretZone
Con la password che trovi su ogni numero della rivista, puoi accedere all'area riservata del sito, con gli arretrati, gli sfondi per la scrivania e strumenti utili.

News e articoli
Leggi le ultime novità, e se vuoi inserisci qui i tuoi articoli: chi ti offre tanto?

Forum
Per esprimere un'opinione, chiedere un consiglio, o semplicemente dialogare con gli altri utenti.

Chat
Puoi accedere direttamente al canale #hackerjournal su irc.azzurra.org, senza bisogno di programmi extra.

Links
Una selezione dei migliori siti sull'hacking, e tutti i siti segnalati dai lettori.

Sondaggio
Partecipa ai nostri sondaggi, dì la tua opinione e guarda i risultati.

ADSL FERMA AL PALO

In Europa c'è ancora molto, troppo scetticismo nei confronti della banda larga. Questi, in sunto, i risultati ottenuti dalle ricerche di mercato effettuate da Jupiter Research, che ha constatato che la maggioranza degli utenti Internet europei vedono molto lontano nel tempo un loro passaggio a Adsl (30%) o non lo considerano per nulla (25%). Sommato a un 20% di incerti e a un 26% di generici "interessati", e confrontato con l'8% di utenze broadband attualmente attive in Italia, il quadro che ne risulta non è certo dei più rosei. O forse semplicemente i tempi non sono ancora maturi…

VIRUS RORON IN AGGUATO

Un bollettino di Kaspersky Labs annuncia la diffusione dell'ennesimo virus trasmettibile via email, denominato Roron. Il virus si diffonde con email che hanno titoli e testi casuali, e allegati infetti che propagano l'infezione una volta eseguiti. Ma, a differenza dei suoi classici predecessori, ha un campo d'azione non limitato alla posta: si copia in tutte le cartelle condivise, diffondendosi quindi nel corso degli scambi P2P, installa una backdoor in mIRC e una base per condurre attacchi DoS, e cancella file a caso il 9 e il 19 del mese. Un virus potenzialmente letale, ma di diffusione limitata. Al momento, perlomeno…

VULNERABILITÀ NELLE PASSWORD DI WINDOWS

E' stato recentemente scoperto un problema piuttosto serio nelle password utilizzate per condividere una cartella in rete sotto Windows 95/98/Me. In poche parole, il server verifica la correttezza di una password, ma non la sua lunghezza; quindi, se viene tentato l'accesso con una password di un solo carattere e questo casualmente corrisponde al primo carattere della password effettiva, l'accesso viene consentito.
Esiste comunque un bollettino Technet riguardante il problema, e comprendente la relativa patch, reperibile presso

www.microsoft.com/technet/security/bulletin/ms00-072.asp.

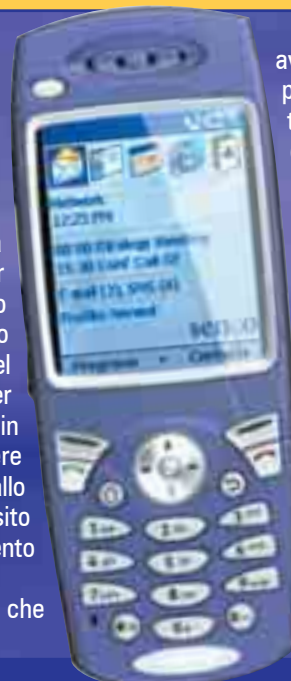
SPEZZATA CHIAVE A 109 BIT

Ci sono voluti diecimila computer, all'opera per 549 giorni, per compiere un'impresa che ha quasi dello storico: vincere la sfida di cracking lanciata nel 1997 da Certicom, azienda canadese che produce software di cifratura per il wireless.
A chiunque avesse "spezzato" i loro codici, Certicom avrebbe corrisposto la considerevole somma di diecimila dollari. E qualcuno ce l'ha fatta. Il vincitore, curioso a dirsi, è un matematico, Chris Monico, ricercatore in una università statunitense, che ha preso la sfida come un problema matematico, e come tale lo ha affrontato e risolto, battendo gli oltre 240 gruppi di lavoro che avevano tentato prima di lui, e che comprendevano a loro volta matematici, esperti di crittografia e informatici, per un totale di circa diecimila persone coinvolte.
C'è da precisare, per tranquillizzare gli utenti dei sistemi Certicom e dei sistemi di crittografia in generale, che il codice crackato è quello di una sola chiave di un singolo utente a 109 bit, mentre, tengono a specificare da parte di Certicom, i codici standard partono da 163 bit, una codifica circa 100 milioni di volte più difficile da violare. Ciò non toglie che l'impresa di Chris Monico sia stata decisamente notevole...

LINUX DAY 2002

Il prossimo 23 novembre, con il patrocinio di Ils (Italian Linux Society), associazione senza scopo di lucro che da quasi dieci anni si occupa della diffusione del software libero, avrà luogo la seconda edizione del Linux Day, giornata dedicata al sistema operativo del pinguino, e in generale al software Gnu. In vista di tale evento, tutti i Lug (Linux Users Group), le associazioni e i singoli che in Italia si occupano di simili tematiche sono state invitate a organizzare nella propria città eventi, manifestazioni e seminari aperti al pubblico, con lo scopo di promuovere la conoscenza e l'utilizzo di Linux, Gnu e del software libero.
L'edizione 2001, la prima della serie, ha visto la partecipazione di circa quaranta Lug e associazioni locali distribuite sul territorio, con una partecipazione di pubblico più che soddisfacente e interessanti e proficui dibattiti su tematiche tecniche, legali ed ideologiche legate all'utilizzo di sistemi "liberi". E la recente attenzione, anche da parte di aziende e pubbliche istituzioni, verso i sistemi open source, ha incoraggiato il ripetersi di tale iniziativa.
Le informazioni sono reperibili presso www.linux.it/LinuxDay o scrivendo a linuxday@linux.it.

MICROSOFT TRADITA DA SENDO

Completamente a sorpresa, l'azienda inglese produttrice di telefoni cellulari abbandona l'implementazione della piattaforma Windows for Smartphone, annunciando di voler passare all'applicazione della tecnologia Symbian, quella, per intenderci, già largamente in uso sugli smartphone Nokia. E questo alla vigilia del lancio sul mercato del modello Z100, atteso in Italia per questo mese e già virtualmente in fase di prenotazione, dopo essere stato presentato, fra l'altro, anche allo Smau: un laconico annuncio sul sito aziendale comunica ora l'annullamento del progetto.
Una brutta botta per Microsoft, che aveva investito svariati miliardi nella partnership con Sendo e che ora si trova con un ridottissimo campionario di smartphone dotati del proprio sistema operativo. Ma le motivazioni addotte da Sendo sono inequivocabili e per nulla lusinghiere nei confronti della casa di Redmond, facendo sottintendere lacerazioni insanabili fra le rispettive politiche aziendali: la piattaforma Symbian è solida e flessibile, e utilizza standard aperti e tecnologie sviluppate in stretta collaborazione fra le aziende del settore. Al contrario di Microsoft… ma era il caso di specificarlo?

➲ ALTAVISTA SI RIFÀ IL TRUCCO

Il noto motore di ricerca, una volta leader del settore, ma recentemente soppiantato nel suo primato da Google (www.google.com), si rinnova radicalmente, offrendo nuove funzionalità, come la ricerca all'interno dei file Pdf presenti in Rete, nonché quella fra immagini, file audio e video, e la limitazione della presenza commerciale, seguendo la linea di semplicità e efficienza che ha fatto il successo del suo acerrimo rivale.
L'obiettivo è quello di riconquistare la fiducia degli utenti, e tornare ad essere il "motore di ricerca affidabile" di Internet. Per fare ciò, ha abbandonato la complessa e affollata struttura a portale, e ha scelto una home page pulita e chiara, scevra da invadenti inserzionisti (come quella di Google, inutile dirlo). Ha inoltre aggiunto la possibilità di raffinare la ricerca con l'opzione "Maggiore precisione", che si avvale di espressioni del linguaggio naturale, e di effettuare una ricerca guidata attraverso Altavista Prisma, che controlla e sostituisce termini di ricerca per restringere il campo. Da non dimenticare, infine, Babel Fish, il celebre traduttore online, vero e proprio cavallo di battaglia del sito.

➲ TAVOLETTE ALLA RISCOSSA

Sono stati finalmente lanciati sul mercato, dopo lunga attesa, i primi modelli di Tablet Pc, basati sulla non recentissima tecnologia del touch screen, che non ha avuto grandi successi nei suoi precedenti tentativi (si ricordi l'Apple Newton) ma che ora è visto come lo strumento ideale per la consultazione di ebook, riviste e quotidiani in versione elettronica.
Il sistema operativo installato sui Tablet Pc è Microsoft Windows Xp Tablet Pc Edition, ed è stata proprio Microsoft a lanciare, circa due anni fa, questo trend, e a scommetterci sopra. Ora sarà la legge del mercato a emettere la sentenza finale.
L'impressione è quella di avere in mano un grosso palmare (le dimensioni sono quelle di un comune computer portatile), che permette di inserire testo "scritto a mano" e, sempre attraverso lo stilo in dotazione, interagire col sistema (non sempre è presente una tastiera integrata).
Si tratta ancora di prototipi, è bene ricordarlo, e sicuramente non saranno loro, con il riconoscimento ancora imperfetto della scrittura e la rozzezza delle forme, a conquistare il mercato. Ma i produttori confidano nel fatto che saranno la testa di ponte per una vera e propria rivoluzione, nella tecnologia e nelle modalità di utilizzo del computer.

➲ MICROSOFT ABBANDONA LA LOTTA CONTRO LINUX

C'è stato bisogno di assoldare una squadra di ricercatori per giungere a questa conclusione, ma ora Microsoft sa che non gli conviene combattere frontalmente Linux. L'utente medio è infatti generalmente ben disposto verso l'open source e vede positivamente la possibilità di avvalersi di sistemi alternativi a quelli Microsoft. Addirittura, la lotta senza quartiere, a tratti in forma quasi di crociata, condotta da Microsoft contro Linux e compagni rischia di rivoltarsi contro la casa di Redmond, creando un senso di disagio che si tramuta in risentimento verso i persecutori e simpatia verso le vittime, soprattutto quando i persecutori si pongono ripetutamente come aspiranti monopolisti del settore.
Inutile anche addurre motivazioni legate agli effettivi costi di gestione di un sistema, paventando una difficoltà tale nella conduzione di un sistema Linux che, secondo Microsoft, ne fa lievitare i costi fino a farla divenire più oneroso, nel complesso, della gestione di un sistema Windows.
Come Microsoft si muoverà per arginare questa spinosa questione è difficile dirlo, ma il pensiero fa tremare i polsi di molti sostenitori del libero software, che temono una ingerenza del colosso statunitense anche in questo campo…

HOT!

➲ BRIDEX, NUOVO VERMICELLO DA EMAIL

Ancora virus nella posta. Bridex (noto anche con il nome di Braid), si nasconde in un attachment dall'ingannevole nome di "readme.exe" e, come Klez, sfrutta una falla di sicurezza di Windows (IFrame Vulnerability, per cui esiste la patch ma che non tutti hanno applicato) per autoeseguirsi ed infettare il sistema. Quindi si autoinvia a tutti gli indirizzi della rubrica, infettando nel contempo con il virus collaterale Funlove tutti gli eseguibili sul disco, compresi quelli condivisi in P2P (aumentando così la diffusione dell'infezione). La prevenzione si opera installando la succitata patch, reperibile presso

www.microsoft.com/windows/ie/downloads/critical/q323759ie/download.asp.

➲ PATCH PER WINDOWS XP

Due problemi corretti nell'ultima edizione del sistema operativo di Microsoft. Il primo è un bug di Explorer che potrebbe causare problemi al sistema in fase di chiusura delle cartelle, mentre il secondo corregge errori di programmazione relativi alla gestione delle periferiche FireWire. Le due patch sono rispettivamente scaricabili presso:

http://download.microsoft.com/download/whistler/Patch/Q329692/WXP/IT/Q329692_WXP_SP2_x86_ITA.exe

http://download.microsoft.com/download/whistler/Patch/Q329256/WXP/IT/q329256_WXP_SP2_x86_ITA.exe.

➲ NORTON CANCELLA LE MAIL PER ERRORE

Un bug piuttosto fastidioso affligge l'ultima edizione di Norton Internet Security, causando la cancellazione di messaggi di posta elettronica. Gli sfortunati utenti che hanno sperimentato i problemi da esso causati parlano di dozzine di mail cancellate e sostituite dal messaggio "Symantec Email Proxy deleted the following email message", senza indicazioni su mittente e argomento del messaggio in questione. Il bug è comunque già stato corretto e la patch diffusa via Live Update.

HOT!

MOZILLA PIENO DI BUCHI

Attenzione alle versioni del browser precedenti alla 1.0.1: sono presenti svariate falle di sicurezza (ben sei, dice il bollettino), che possono dimostrarsi molto pericolose. I rischi sono quelli di avere il proprio hard disk "visitato" da ospiti non invitati, e i propri dati riservati facilmente accessibili. Uno degli inconvenienti, per esempio, è quello di non essere avvertiti quando si viene reindirizzati da un sito sicuro a un uno non sicuro. La soluzione è una e semplice: aggiornare Mozilla alla versione più recente.

WIRELESS TROPPO POTENTE

E' tornato in questi giorni alla ribalta un annoso problema, quello legato all'utilizzo di periferiche wireless come mouse e tastiere. L'allarme arriva dalla Norvegia, dove un ignaro utente ha visto apparire sullo schermo del suo computer parole che lui non stava affatto scrivendo. Esclusa la presenza di una backdoor o di un virus di qualunque tipo, l'utente ha scoperto che si trattava di ciò che il suo vicino di casa stava scrivendo con la sua tastiera wireless, a 150 metri da lui.

LO SPAM AUMENTA…

…e si fa sempre più impudente, se è vero che, secondo Brightmail, azienda produttrice di software antispam, al sensibile diminuire di spam finanziario, ovvero gli inviti ad aderire a fantomatici programmi di investimento, a vendite multilivello o al recupero delle sostanze di uomini politici nigeriani, fa riscontro un sostanziale aumento dello spam "a luci rosse", con offerte di prodotti, link, immagini o video, che, sommandosi alla presentazione di prodotti di ogni genere e alle classiche "bufale", aumentano sempre più le presenze indesiderate nelle nostre mailbox.

BLU SI RIFUGIA IN WIND

Il provider di telefonia cellulare, travolto dalla crisi e già con le valigie in mano per abbandonare la sua tormentata avventura, passa il suo parco clienti a Wind, che prepara per questi un'accoglienza di tutto rispetto: una sim Wind con piano Easy Wind, Sms gratuiti e chiamate con lo sconto del 50% fino al 31 gennaio 2003, senza cambiare numero di cellulare e senza perdere il credito residuo Blu. Sono stati inviati Sms di invito a tutti coloro che utilizzano regolarmente la scheda Blu, e che in generale hanno effettuato almeno una ricarica negli ultimi mesi. Chi ha già aderito all'offerta ha ricevuto per posta la sim, assieme a un buono omaggio di 5 euro, utilizzabile per la ricarica.
E' per il momento ancora possibile mantenere la propria sim Blu e il proprio profilo tariffario, almeno fino a marzo 2003, secondo le dichiarazioni dell'azienda.Non è dato sapere cosa sarà di coloro che non accetteranno, per qualsiasi motivo, anche se si ventila l'ipotesi di un "passaggio coatto": Blu è comunque destinata a cedere completamente le armi entro un massimo di sei mesi.

AMIGA SI EVOLVE IN AMIGAONE

I processori PowerPc hanno dato nuova vita all'antica e tanto amata macchina, il cui nome strappa ai più maturi sospiri nostalgici e ai più giovani l'emozione dei tempi eroici del pionierismo informatico. Il nuovo sistema operativo, AmigaOs 4.0, per onorare tale dignitosa memoria sarà basato su Linux e ottimizzato per lo specifico processore. AmigaOne sarà presentato a Natale 2002, mentre il sistema operativo sarà pronto nei primi mesi del 2003. Ma i produttori consigliano a chi fosse ansioso di entrare in possesso di un esemplare della mitica macchina di affrettarsi: le prenotazioni stanno già fioccando, e si prevede un reale "tutto esaurito". Inoltre, agli acquirenti "precoci" di AmigaOne verrà recapitata gratuitamente una copia di AmigaOs 4.0, non appena disponibile.
AmigaOne sarà disponibile in diverse versioni, basate su processore G3 e G4: AmigaOneG3-SE (G3 a 600MHz), AmigaOne-XE (G3 a 700MHz) e AmigaOne-XE (G4 a 800MHz). I prezzi vanno dai 580 euro dell'AmigaOneG3-SE ai circa 800 dell' AmigaOne-XE.

NASCE LA COMMISSIONE PER L'OPEN SOURCE

Seguendo il lodevole esempio della Comunità Europea, nell'ambito del Ministero per l'Innovazione e le Tecnologie è stata creata una "Commissione per il software a codice sorgente aperto nella Pubblica Amministrazione". Tale commissione è sorta principalmente per valutare i modelli, i costi e l'impatto del software libero sulle strutture della Pubblica Amministrazione, dopo la dichiarazione di intenti del ministro Stanca in tal senso, la scorsa estate.
L'operato della Commissione si concentrerà sulla verifica di alcuni punti inprescindibili, come il contenimento dei prezzi, la sicurezza, la reperibilità, l'accessibilità a tutti i livelli dell'amministrazione, centrale e locale. Ovviamente da qui a dire che tutte le macchine della Pubblica Amministrazione gireranno sotto Linux il passo è molto lungo, considerando soprattutto i tempi e i modi di elaborazione di questo genere di cose, ma questo è senz'altro un evento importante, per chi si occupa di Open Source e crede profondamente nella sua utilità ed efficacia.

PALM E LE TASTIERE

Palm ha acquistato la licenza delle tecnologie che sono alla base delle minitastiere di Research In Motion (Rim) e che costituiscono il punto di forza di Tungsten W, il primo Palm smartphone e con tastiera incorporata. Questa notizia segna la fine di una lunga battaglia giudiziaria che ha visto Palm sul banco degli imputati per l'utilizzo improprio delle tecnologie di Rim. Anche Handspring si era trovata dalla stessa parte della sbarra, per le tastiere utilizzate per i Treo e non licenziate da Rim.

Questa iniziativa è tanto più importante quanto la si ricollega alla crescente importanza che stanno avendo ed avranno nell'immediato futuro le tastiere per Pda e Smartphone: questi dispositivi sono sempre meno da considerarsi agende sottousate o telefonini ipertrofici, e sono sempre più veri e propri strumenti di lavoro, che necessitano di un sistema rapido e pratico per immettere velocemente grandi quantità di dati, compito a cui il sistema di riconoscimento Graffiti o le tastiere touchscreen non possono più sopperire.

NUOVI PORTATILI DA APPLE

Nuovi ed economici, potremmo aggiungere. Ed è forse questa la vera novità: accanto al potenziamento dei processori (da 700/800 MHz per l'iBook fino a 1 GHz di clock per il Titanium), delle schede video (Radeon Mobility da 16 a 64 Mbyte) e dei dischi rigidi (fino a 60 Gbyte sempre per il Titanium), vediamo scendere l'iBook base sotto la famigerata soglia dei mille dollari (circa 1300 euro per l'Italia). E parliamo comunque di un portatile piccolo e leggero, con modem, scheda di rete Ethernet, ingressi Usb e FireWire e addirittura la predisposizione per il Wireless Airport. E comunque il top della serie, il Titanium G4, non supera i 4000 euro, 1500 euro almeno in meno delle precedenti teste di serie, e ha in più il Superdrive per masterizzare i Dvd, che lo rende una vera e propria stazione di produzione video portatile.
Con queste nuove linee Apple si allinea ai prezzi dei portatili Wintel, con in più il tocco di qualità che li contraddistingue.

CD AUDIO PROTETTI: È GUERRA APERTA

Le major della discografia fanno orecchie da mercante alle critiche, anche autorevoli, contro la discutibile pratica della protezione dei CD audio. Discutibile non tanto per il principio in sé, ma per i problemi ad essa correlati. Dall'impossibilità di riprodurre i supporti nel lettore del computer, ad altri malfunzionamenti vari causati da imperfetta applicazione del logaritmo di blocco, la protezione ai Cd davvero non va giù. Nonostante questo, uno dei più grossi gruppi del settore, Bertelsmann Music Group (Bmg), ha annunciato che adotterà dispositivi anticopia in tutti i Cd musicali prodotti. E pare che Emi sia fermamente intenzionata a fare la stessa cosa. Passando al contrattacco: Bmg ha realizzato una guida online sui Cd protetti e il perché sia giusto adottare tale tecnologia (difesa del diritto d'autore, impedire alla pirateria musicale di togliere risorse economiche che sarebbero altrimenti dedicate a promuovere nuovi talenti, e via dicendo). Si dice inoltre che le nuove tecnologie di protezione saranno assolutamente scevre da problemi, e non limiteranno in alcun modo l'ascolto, riconoscendo quindi la presenza di problemi sugli attuali Cd protetti. Ciò che non prende in considerazione Bmg è se tutto questa attenzione ad impedire la copia non allontanerà ancora di più gli acquirenti dagli scaffali dei negozi, col timore di acquistare un prodotto in qualche modo “limitato”…

SMS SOLIDALI

Tim ha invitato i propri clienti a esprimere solidarietà alle popolazioni colpite dal terremoto in Molise, inviando un Sms al numero 4466. Il messaggio, del costo di un euro, permetterà di devolvere quell'euro alla causa dell'assistenza e della ricostruzione nelle zone terremotate.
Wind ha subito seguito l'esempio, mettendo a sua volta a disposizione un numero di telefono da chiamare per devolvere un euro alla stessa causa. I numeri da chiamare sono 434343 da cellulare Wind o 1088434343 / 1055434343 da linea telefonica fissa.

MOVIELINK PER I FILM IN RETE

È stata costituita una joint venture fra Mgm, Paramount Pictures, Sony Pictures Entertainment, Universal e Warner Bros che, in partnership con Microsoft and RealNetworks, lancerà un servizio di “proiezione” di film sul Web. Tale iniziativa vorrebbe essere una risposta alla pirateria cinematografica, che in tempi recenti ha affiancato quella musicale, grazie al diffondersi di nuove tecnologie. Ma i problemi che Movielink si troverà ad affrontare sono seri e ben noti: richiesta limitata, tecnologia ancora non adeguata e problemi legali.

UMTS DI TIM ENTRO FINE ANNO

Per smentire tutte le voci che vogliono Umts come un progetto troppo ambizioso, fermo al palo ancora prima di essere stato davvero lanciato, Tim ha confermato che entro l'anno partiranno i propri servizi Umts, e che potranno già contare su qualche migliaio di utenti, grazie alla buona copertura di partenza. Si parla di circa mille antenne nelle principali città italiane, e un potenziale di decine di migliaia di cellulari Umts in circolazione entro fine anno.

HJ ha surfato per voi...

I classici della Rete

www.antionline.com

AntiOnline contiene migliaia di programmi in archivio, migliaia di testi sulle tematiche della sicurezza, accesso a tutti i principali newsgroup relativi alla sicurezza, un forum ricchissimo e una chat ben frequentata. È possibile personalizzare l'aspetto del sito in base alle proprie esigenze e ai propri interessi, e persino avere un sottodominio *.AntiOnline.org. Decisamente non si tratta di un sito in cui fare una veloce visita e basta.

http://freaky.staticusers.net/ugboard

Dall'url non si intuisce l'argomento di questo sito/forum, ma basta guardare il banner per capire al volo: Macintosh Underground. Tutto quello che riguarda il lato oscuro della mela, dalla sicurezza dei sistemi Mac classici e Mac OS X alle procedure per rippare, convertire e masterizzare DVD; dalla crittografia a una lista di indirizzi per Hotline, Carracho, FirstClass & Co. Il sito principale è in inglese, ma una sezione è interamente in lingua italiana.

15 minuti di celebrità! Questi sono i vostri

www.evaicomunications.cjb.net

Alcune sezioni sono ancora in allestimento ma io gli darei un'occhiata, dato che stiamo per inserire alcuni kernel alternativi ai 3 "BIG": Windows, Linux e Mac OS. Saranno presenti anche molti programmi da scaricare (prevalentemente in GPL), e molto altro. Ci sono anche le news e, mi raccomando, FIRMATE IL GUESTBOOK e RIEMPITE IL FORUM!!!!

Massimo

http://digilander.libero.it/securitynet

Ciao carissima redazione di hacker journal, volevo solo chiedervi di mettermi tra i vostri link.
Anticipo i ringraziamenti e a risentirci.

ski net

siti; scegliete voi se tirarvela o vergognarvi

http://digilander.libero.it/esystem

Sono un giovane WebMaster (16 anni) e volevo sfidare quel pizziko d fortuna che per ora mi sento addosso. Vorrei infatti (sarebbe strepitoso) che mettereste il mio sito sulle pagine di Hacker Journal, perché credo che il mio ultimo sito sia molto carino.

FUEL, hck group

www.pcware.tk

Siamo una crew che nasce per espandere le conoscenze di ogni membro nel campo informatico....
Ci interessiamo principalmente di Hacking in generale, di sicurezza e soprattutto di programmazione. Stiamo sviluppando diversi programmi utilizzando il Visual Basic e il C.

Pc-Ware

http://guide.supereva.it/database/sicurezza

Vi scrivo per segnalare la sezione della mia guida sui database, dedicata alla sicurezza.
Invito inoltre chiunque abbia un sito che tratta argomenti legati alla sicurezza dei database a segnalarmelo.

Andrea

I classici della Rete

www.oth.net

Prima di AudioGalaxy, prima di Gnutella, prima di Hotline e Carracho, Prima ancora di Napster, c'era Oth.net. Si tratta di un motore di ricerca per siti ftp. Il procedimento è simile a quello del peer to peer, ma un po' più laborioso: si mette su un server ftp sulla propria macchina, si comunica l'indirizzo a oth.net, e questo inserirà la lista dei file presenti nel suo motore di ricerca, accessibile direttamente dalla home page del sito.

www.arstechnica.com

Volete sapere quali sono le differenze tra un Pentium IV e quella di un Athlon? O come si possono confrontare le prestazioni di processori con architettura diversa (CISC/RISC)? Eccovi un sito tutto dedicato a notizie e informazioni tecniche sui processori, con un occhio di riguardo a tutte le pratiche che servono ad aumentare le prestazioni del proprio computer, overclocking incluso.
Alcuni documenti sono decisamente approfonditi e riservati ai lettori più tecnici: per molti, ma non per tutti.

SINDROME CINESE

Spam, hacker di stato, guerra digitale e spionaggio di massa: gli inquietanti aspetti delle attività informatiche del più popolato paese al mondo

LA CINA E INTERNET: UNA RELAZIONE POTENZIALMENTE PERICOLOSA

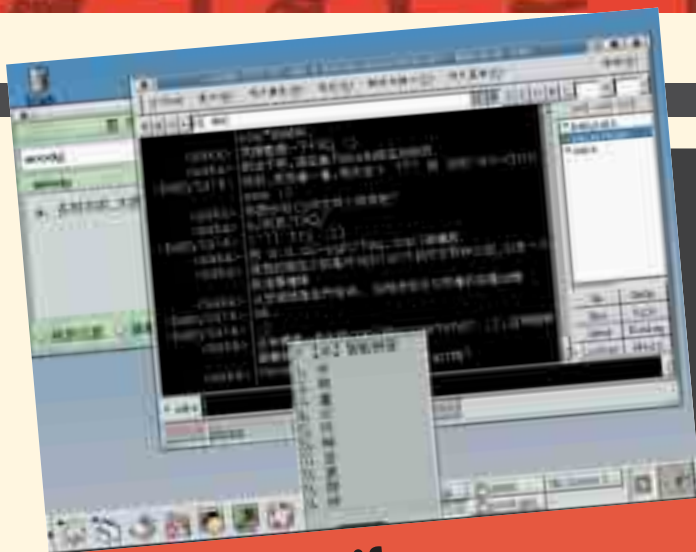
È la notte tra sabato 31 marzo e domenica primo aprile 2001. Una telefonata butta giù dal letto il vicepresidente americano, Dick Cheney: è lo stato maggiore della marina. Un nostro aereo spia, spiega l'ammiraglio Houstbound, è stato abbattuto dai cinesi poche ore fa.

In realtà **l'aereo, un grosso quadrimotore Ep-3, 24 uomini di equipaggio, dotato dei più aggiornati sistemi di sorveglianza elettronica (leggi "spionaggio") è stato intercettato a sud dell'isola di Hainan, nel Golfo del Tonchino** (10 Km a sud secondo i cinesi, 110 Km secondo gli americani). Una ricognizione di routine partita dalla base dell'Air Force di Okinawa, in Giappone, che all'improvviso diventa un dramma. Due caccia cinesi affiancano l'aereo americano. L'Ep-3 tenta una manovra evasiva, ma il veivolo "tocca" uno dei due caccia (che cade provocando la morte di Wang Wei, il pilota) e -danneggiato- è costretto ad atterrare nella base militare cinese di Hainan.

Bush, neoeletto presidente degli Stati Uniti, fa subito fuoco e fiamme, ma la Cina non si lascia impressionare: dall'altra parte c'è qualcuno più "duro" del presidente texano. E' Jiang Zemin, considerato un "duro" anche dai generali delle forze armate cinesi. Saranno 11 giorni di tensione: da una parte gli Usa che rivogliono indietro i loro uomini e - soprattutto - la tecnologia contenuta nel loro gioiello volante per lo spionaggio elettronico; dall'altra la Cina, che pretende giustizia e risarcimenti per la violazione del proprio spazio aereo e per la morte del suo pilota (oltre a voler curiosare tra le tecnologie americane).

Mentre una flottiglia di tre navi americane da guerra si avvicina al Mar Cinese meridionale, sul tavolo diplomatico i cinesi calano l'asso: per riavere l'aereo gli Usa si devono impegnare a non vendere a Taiwan (la Cina nazionalista, in lotta contro la Cina continentale comunista dalla fine della Seconda guerra mondiale) le nuove tecnologie antimissile, che limiterebbero le capacità offensive cinesi in caso di conflitto con quel paese. Alla fine, sarà un compromesso diplomatico a sbloccare la situazione.

>> Nel frattempo, sulla rete...

Tuttavia negli stessi giorni si sta svolgendo una guerra silenziosa che in pochi hanno documentato. Tra il 2 aprile e il 9 dello stesso mese, secondo un rapporto riservato della sezione per la sicu-

La Cina in cifre

1,3 miliardi di abitanti
9.596.960 chilometri quadrati di superficie
33,7 milioni di utenti Internet
12 milioni di Pc venduti nel 2001
90 milioni di telefoni cellulari
200 milioni di linee telefoniche
Lingue parlate: il 91,9% della popolazione parla il Cinese Standard o Mandarino, derivato da un dialetto di Pechino, oppure il Cantonese (Yue), il dialetto di Shangai (Wu), il Minbei (Fuzhou), il Minnan (Taiwan), Xiang, Gan, vari dialetti Hakka. Inoltre, le minoranze etniche (pari all'8,1% della popolazione) parlano i dialetti Zhuang, Uygur, Hui, Yi, Tibetano, Miao, Manchu, Mongol, Buyi e Coreano.

Come dite "spam" a Pechino?

Una enorme quantità di messaggi pubblicitari non desiderati (spam) in circolazione oggi giorno arriva in un modo o nell'altro dalla Cina. In parte si tratta di messaggi spediti dalle nascenti imprese private cinesi, in caccia di relazioni commerciali con aziende straniere (per lo più americane); questi messaggi sono spesso scritti in un inglese molto scarno, se non addirittura in una delle lingue cinesi. Non avvezzi all'uso della rete e ignari della netiquette, orde di imprenditori stanno tempestando gli occidentali di messaggi che, nel migliore dei casi, faranno irritare i potenziali clienti invece che invogliarli.
Più simile a quello che conosciamo abitualmente è invece lo spam che, pur originando da siti e aziende occidentali, viene in realtà spedito appoggiandosi su server di posta cinesi. In questo caso è spesso difficile per il normale utente risalire al server di origine analizzando l'header di posta, ma gli stessi provider hanno problemi a gestire l'enorme mole di messaggi che arrivano dalla Grande Muraglia. Alcuni osservatori sostengono che i server Smtp cinesi sarebbero molto poco protetti, e verrebbero quindi sfruttati illegalmente dai veri "mandanti" dello spam. Nessuno, insomma, avrebbe veramente intenzione di inviare spam… Quello che però questa teoria non spiega è come mai, in un sistema così regolamentato e controllato, nessuno si sia mai preoccupato di identificare e redarguire gli amministratori dei server che inviano così tanti messaggi. Vogliamo scommettere su cosa accadrebbe se l'oggetto dello spam fosse un sito fortemente critico verso il Governo cinese?.

rezza informatica del Dipartimento di Stato americano, avvengono **circa 412 attacchi informatici "particolari"**. Da un lato, sconosciuti e **abili esperti informatici americani compiono circa 387 intrusioni di "elevato livello e capacità tecnologica" all'interno di siti cinesi**, per proclamare il proprio patriottismo. Dall'altro, **"pirati cinesi hanno compiuto almeno 25 violazioni informatiche" di sistemi statunitensi, tra i quali il Dipartimento del Lavoro e quello della Sanità.**

Non è la prima volta che la Cina diventa protagonista di quello che viene definito CyberWarfare, la guerra elettronica. E' la temuta minaccia della "Pearl Harbor digitale", analizzata negli Stati Uniti dagli esperti militari di sicurezza e diventata presto la scusa ufficiale per la caccia agli hacker (soprattutto americani ed europei) in corso dalla fine degli anni ottanta.
Ma la Cina e gli altri paesi dell'Estremo Oriente rappresentano davvero soltanto un pericoloso nemico? A giudicare dagli interessi economici che soprattutto gli Stati Uniti hanno in quell'area, si direbbe di no. Alla fine del 2001 la Cina è entrata nell'Organizzazione mondiale del commercio, ed è considerata il mercato destinato alla maggiore espansione anche e soprattutto in campo elettronico. Un intero continente, **popolato da un quinto della popolazione mondiale** (1,3 miliardi di persone), con soli 12 milioni di Pc venduti nel 2001 e 33,7 milioni di utenti Internet (il doppio dell'Italia), che del 50 per cento all'anno. Una vera manna, rispetto agli agonizzanti mercati tecnologici occidentali.
Insomma, considerando la cosa dal punto di vista industriale delle grandi aziende produttrici di tecnologia, la Cina vive una situazione unica: coesistono vecchie e nuove tecnologie, si incrociano satelliti, internet, telefonia cellulare, fibre ottiche e infrastrutture militari. Ma gli utenti sono ancora pochissimi e il costo del lavoro è estremamente basso. Chi vince la sfida del mercato cinese, vince in tutto il mondo. Chi perde, perde in tutto il mondo.

Tuttavia la Cina non si è aperta alle tecnologie occidentali e all'arrivo delle grandi multinazionali senza organizzarsi per difendere il suo regime interno.

>> Una rete a maglie strette

La legislazione prevede limiti di vario genere all'apertura di nuove fabbriche con capitale occidentale, che devono avere il nulla-osta del governo di Pechino, e l'accesso a Internet da parte della popolazione è sottoposto a una serie di regolamentazioni che in Europa non sono neanche immaginabili.

Da due anni, infatti, c'è la **pena di morte per chiunque sia riconosciuto colpevole di essersi appropriato o di avere divulgato documenti di stato** - quindi coperti dal segreto - su Internet.
Inutile dire che il concetto di "documento di stato", ancorché coperto dal segreto, è interpretabile in modo abbastanza ampio, e qualunque cittadino cinese che

Six/Four: comunicazione anonima e sicura

Fidonet e FredNet, ma anche le reti di base. La filosofia dietro alle grassroots non è nuova, ma si sviluppa dopo il 4 luglio 1989, il giorno dei massacri di Piazza Tiananman, una delle pagine più nere della storia cinese recente. Il gruppo di hacker Hacktivismo, spin-off del collettivo Cult of the Dead Cow, decide di realizzare un protocollo che permetta di navigare, chattare e scambiare file ed email senza lasciare alcuna traccia. Una forte minaccia per la sicurezza, si direbbe oggi, in realtà l'unica forma di sicurezza possibile per chi viva in un paese dove il regime cerca di intercettare e censurare tutte le forme di comunicazione, anche quelle elettroniche. Alla base tecnologica del protocollo, Six/Four, c'è un mix di Vpn, tunneling, approccio peer-to-peer e open-proxy. Maggiori dettagli verranno rilasciati a breve sul sito hacktivismo.com, in cui però già si può trovare una versione funzionante di Camera/Shy, software di steganografia che permette di nascondere messaggi cifrati dentro a normali immagini.

Il principale autore del protocollo è The Mixter, un hacker tedesco rintracciabile all'indirizzo mixter.void.ru. Mixter, che è un personaggio noto nell'ambiente hacker, è anche l'autore di Tribe FloodNet, un programma utilizzato spesso per effettuare attacchi dDoS.

mandi un email all'estero contenente informazioni considerate "segrete" (o magari "politiche" e "democratiche") rischi in effetti la pena capitale. Oltretutto in Cina, secondo Amnesty International, le esecuzioni non sono affatto un fenomeno raro.

>> The great (fire)wall of china

Dal primo agosto di quest'anno, inoltre, **in Cina è in vigore una legislazione che limita fortemente il numero e la struttura dei gestori di siti, portandoli direttamente sotto il controllo governativo**.

Come se non bastasse, negli ultimi due anni si sono succeduti gli episodi di censura da parte del governo cinese nei confronti di Internet: i provider locali sono stati costretti a impedire l'accesso a intere serie di indirizzi Ip, **nel 2001 è stato impedito l'accesso a Freenet** (servizio Ftp e di scambio informazioni senza censure) **e ai principali motori di ricerca** (Google, Altavista, Yahoo etc.). Ancora, in tre differenti riprese il governo ha chiuso gli Internet Café della capitale, punto di accesso per la grande massa di studenti che frequenta Pechino e che non può permettersi un Pc e un collegamento ad Internet. In altre zone, per accedere agli Internet Cafè bisogna registrarsi presso la polizia e ottenere un tesserino di riconoscimento, che permette di **tracciare e registrare ogni attività compiuta online dai cittadini**.

Senza contare l'installazione di **sistemi analoghi a quello americano di Carnivore: box dedicate al filtraggio dei pacchetti Tcp/Ip installate per legge presso i server di tutti i fornitori di accesso**. Negli Usa, nonostante l'11 settembre, la questione è ancora discussa; in Cina è una certezza matematica.

Insomma, se in passato la Cina si è difesa dai mongoli con la Grande Muraglia, ora il governo vorrebbe che il paese si trasformasse in **un'enorme Intranet chiusa da un Firewall**, e i cui contenuti siano strettamente controllati. Per fare questo, lotta anche contro le principali aziende produttrici di software: da circa un anno e mezzo sono in corso le **sperimentazioni per basare le infrastrutture cinesi su server e desktop in ambiente Linux**. L'idea è che in questo modo è possibile rendersi autonomi da Microsoft e dalle politiche di "sicurezza" che il sistema operativo di Microsoft sta realizzando sotto la spinta anche del governo statunitense. Avere una infrastruttura non basata su Windows significa non essere esposti, in caso di guerra commerciale o elettronica, al rischio che il potenziale nemico, gli Usa, sia anche il possessore di una delle risorse fondamentali: il sistema operativo dei propri computer.

>> Vita dura per gli hacker

Ma la scena hacker dell'Estremo Oriente non è per questo meno vitale di quelle occidentali, anche se fortemente inquinata dall'**onnipresente governo, che cerca anche di arruolare i migliori talenti**.

Difficili da individuare, spesso parte di movimenti politici antagonisti del regime di Pechino, gli hacker cinesi nascono soprattutto vicino ai grandi centri universitari del paese, come Hebei, Yenching, Tsinghua, Chaoyang, Soochow, Xiamen, Wuhan, Hunan, ma anche nelle aree di maggiore industrializzazione tecnologica, come Shangai e Hong Kong.

La loro presenza è avvertita come una

minaccia nazionale, e abbiamo visto che in alcuni casi **questo può anche tradursi in condanne durissime, persino nella pena capitale**. Durante gli ultimi mesi sono stati arrestati almeno 15 "sospetti hacker", a partire dall'arresto nel distretto di Haidian (Pechino) a maggio dell'anno scorso di Lu Chun, **un ventunenne colpevole di aver rubato un paio di account da un'azienda e averli utilizzati per navigare su Internet** (e far navigare qualche suo amico), sino all'arresto del diciassettenne Chi Yongshu, studente di liceo nella provincia di Heilongjiang (nel nord-est del paese), colpevole questa volta di **reati più complessi: diffusione di virus, furto di dati e traffici illeciti online**. Infine, un 36enne impiegato di un istituto di credito (Banca della comunicazioni della Cina), **accusato di aver rubato dai conti correnti dei propri clienti quasi due milioni di yuan** (200 mila dollari) a partire dall'agosto del 1990, dopo che era fuggito in Canada solo per essere espulso dalle autorità di quel paese, **è stato condannato a morte e giustiziato.**

Gli hacker, anzi "heike", come viene tradotta foneticamente l'espressione inglese in cinese, comunque ci sono. E non sono solo ladruncoli, ragazzini che giocano con le password o soldati della cyberarmata di Pechino. Vari gruppi di hacker europei e statunitensi, che ultimamente hanno ribadito di non essere coinvolti con gli attacchi che dall'occidente vengono sferrati ai nemici degli Stati Uniti come Cina, Corea del Nord e Irak (l'ultima a dichiarare la sua estraneità è stata Legion of Underground), nel tempo hanno anche stabilito contatti forti con i loro colleghi cinesi. Alle volte, il contatto ha voluto dire un aiuto sostanziale.

La comunità hacker internazionale, infatti, sensibile - com'è ovvio - al tema di poter garantire la propria privacy nei confronti di regimi oppressivi, ha offerto soluzioni per chi vive in paesi come la Cina: software come Camera/Shy di Hacktivismo e Six/Four per la creazione di reti grassroot assolutamente anonime, sono regali pensati non per fornire nuove armi ad hacker "cattivi" e terroristi stranieri, ma **per permettere l'esercizio dei più elementari diritti democratici anche a chi vive in paesi dove questo non è concesso**.

Dalla Cina, a parte hacker etici e combattenti per la democrazia, arriva anche molto di più che non il solo virus dell'influenza autunnale. **Ogni anno si contano almeno una decina di "ceppi" virali informatici provenienti (o presunti tali) dall'Estremo Oriente**. Ad esempio, il worm 1i0n. I mass-media, abituati a fare di ogni erba un fascio già con il termine hacker, sul "pericolo giallo" ci sguazzano letteralmente. Eppure, la guerra sotterranea tra presunti hacker occidentali (soprattutto americani) e cinesi continua. Di dimensioni molto ridotte rispetto al conflitto tra "pirati" filo-israeliani e "pirati" filo-palestinesi, il bombardamento a colpi di defeacement è tuttora in corso. Forse in Cina anche con l'approvazione governativa, se non proprio con il suo stesso impegno. Gruppi come The Honker Union of China (Honker è una delle espressioni slang cinesi per hacker) hanno dichiarato di voler combattere "l'arroganza anti-cinese" con tutti i mezzi. Anche con 80 defeacement consecutivi e la compromissione di altri 400 server.

aDm

Pechino contro la Rete del Dalai Lama

"We are definitely under attack. This is not paranoia. Something very weird is going on, BEWARE", così iniziava, sabato 20 aprile 2002, la preoccupatissima e-mail di Antony OBrien, uno dei più assidui frequentatori di Tibet Support Groups-List (TSG-L), la principale rete internazionale di tibetani e sostenitori della lotta del popolo tibetano contro l'occupazione cinese del Paese delle Nevi. Cosa stava succedendo di così grave? Come divenne chiaro nel giro di poche ore, alcuni hackers cinesi erano riusciti, grazie a una sventagliata di virus Trojan, ad impadronirsi dei impadronirsi dei computers di alcuni dei più noti animatori della lista e, attraverso e-mails inviate a loro nome, entrare in decine di altri computers di iscritti alla TSG-L. Fatti esaminare da esperti di Symantec e Mcafee, questi virus sono risultati estremamente sofisticati e inviati da Pechino e da altre città della Cina Popolare. Anche se il governo cinese ha ufficialmente negato di aver a che fare con questo attacco massiccio e coordinato, i tibetani e i loro amici sono assolutamente convinti che sia impossibile in un Paese come la Cina, dove vige il più totale controllo governativo su tutti gli aspetti della comunicazione, per la comunità degli hackers (che peraltro è in genere tutt'altro che favorevole al regime) impostare un'operazione così ben articolata e prolungata nel tempo. Tra l'altro tutte le reti collegate ai diversi aspetti del dissenso cinese (sindacalisti clandestini, intellettuali, aderenti alla Falun Gong, etc.) hanno comunicato alla TSG-L di essere sottoposte anch'esse ad analoghi attacchi. Adesso la TSG-L sta cercando di attrezzarsi per rispondere all'emergenza perché è chiaro che anche sul Tetto del Mondo e nel remoto oriente ormai i veri giochi si fanno sulla Rete.

Piero Verni

CINQUE DISTRIBUZIONI LINUX A CONFRONTO

I MILLE VOLTI DEL PINGUINO

Chi si avvicina per la prima volta a Linux si trova subito di fronte a un dubbio: quale scegliere tra le decine di distribuzioni possibili?

Linux Links

Non potete non visitarli!
http://www.kernel.org
http://www.gnu.org

Ma quante distribuzioni esistono?
http://www.linuxlinks.com/Distributions/
http://old.lwn.net/Distributions/
http://www.linux.org/dist/index.html

Scaldate il vostro masterizzatore...
http://www.linuxiso.org/

Linux in realtà è il nome del kernel cioè del "cuore", della parte fondamentale del sistema che svolge le funzioni fondamentali come la gestione dei dispositivi o dei processi; torneremo in futuro su questo argomento ma, per il momento, vi basti sapere che **Linux è semplicemente una parte dell'intero sistema**. Tuttavia è evidente che per utilizzare un computer è necessario avere anche tutto un corredo software adeguato; una shell a riga di comando e i principali tool per l'utilizzo del sistema, un compilatore C e inoltre editor di testi, giochi, interfacce grafiche e tutto quant'altro può servire. Le primissime versioni di Linux utilizzabili consistevano in un paio di floppy: un disco di avvio contenente il kernel e un disco di root per l'utilizzo del sistema contenente i basilari tool sviluppati negli anni precedenti proprio dal progetto GNU (fondato da R. Stallman). Ecco quindi che l'accoppiata GNU/Linux indica un sistema operativo di base pienamente funzionante e utilizzabile. Tuttavia la configurazione del sistema era ancora complessa e completamente manuale; col tempo però diverso software iniziò ad essere portato con successo su Linux e **ben presto i tempi divennero maturi e naquero le prime distribuzioni**. In pratica una distribuzione Linux non è altro che una combinazione del sistema di base GNU/Linux e di una selezione del software disponibile a cui vengono aggiunti degli strumenti per l'installazione e la configurazione del sistema e della specifica documentazione.

>> In cosa differiscono tra loro?

Esistono moltissime distribuzioni e **ciascuna è diversa dalle altre per numero e scelta dei programmi e delle librerie allegate, così come diversi sono i vari strumenti per l'installazione e la configurazione del sistema o del gestore di finestre** (notoriamente ostico), o ancora le piattaforme supportate (non solo Intel-compatibili ma anche Alpha, Sparc, PowerPC...). Inoltre molto spesso il sistema è localizzato, viene fornita della documentazione (in formato cartaceo o elettronico) così come può essere incluso un servizio di assistenza per l'installazione; infine il sistema di gestione dei pacchetti software (che consente di installare, aggiornare o rimuovere con facilità le applicazioni) non è sempre il medesimo così come molto spesso molti file del sistema vengono posizionati in directory diverse.

>> Quale mi conviene utilizzare?

Una domanda come questa sarebbe in grado di scatenare vere e proprie guerre di religione in qualsiasi chat, forum, mailing-list o newsgroup! :) In linea di massima occorre **considerare le mansioni che la nostra Linux-box dovrà svolgere** (server, workstation, firewall...), l'aggiornamento del Kernel e dei suoi componenti principali quali il compilatore C o XFree (e ricordate che una distribuzione chiamata Foo 8.0 non è necessariamente più recente di una Bar 4.3, ma che soprattutto avere sempre l'ultima versione installata non è necessario), la qualità dei tools di installazione, dei manuali o dei servizi offerti e così via. Il consiglio è comunque sempre uno: provate e decidete voi stessi! Noi **abbiamo analizzato per voi cinque distribuzioni per processori x86 e una per Power PC**: nelle prossime pagine troverete le nostre valutazioni.

Lele
www.altos.tk

Perché dovrei pagare se GNU/Linux è libero?

Libero non vuol dire gratuito; inoltre occorre premettere che non tutte le distribuzioni sono commerciali e pertanto una distribuzione come Debian rende disponibili per il download le immagini ISO per l'intero set di CD. Altre si limitano a rendere disponibili soltanto una versione di base (contenente pertanto una selezione dei pacchetti). Inoltre, benché i sorgenti di Linux e della maggior parte delle applicazioni per questo sistema possano essere liberamente scaricati da Internet, la preparazione di un intera versione e dei relativi programmi di installazione richiede tempo per essere sviluppata e aggiornata. Se poi consideriamo i costi per la stampa e la traduzione dei manuali, l'assistenza spesso offerta o anche solo il tempo risparmiato a cercare, scaricare e talvolta compilare pacchetti su pacchetti...

Debian GNU/Linux 3.0

debian

www.debian.it
Versioni: Debian GNU/Linux 3.0 (€ 24,00, 7 CD)
Kernel: 2.4.18
Facilità d'uso: **
Completezza: ***
Sicurezza: *****

Debian è l'unica tra le "grandi" distribuzioni a non dipendere da una struttura commerciale e ad avere come unico fine lo sviluppo di software libero. Lo scopo primario di questo progetto è pertanto lo sviluppo di una distro estremamente sicura e stabile (oltre che disponibile per molte piattaforme). Questa ricerca di qualità implica tuttavia tempi di sviluppo lunghissimi e criteri per la scelta dei pacchetti estremamente selettivi. Tanto per fare un esempio, in Debian 3.0 (stable-release ufficiale) i "grandi assenti" sono proprio KDE 3, GNOME 2 o XFree86 4.2! Inoltre, l'installazione (solo in modalità testuale) è piuttosto laboriosa e non sempre intuitiva. Il sistema di gestione e aggiornamento (apt) dei pacchetti DEB è il migliore tra quelli diffusi in ambito GNU/Linux, e l'ambiente grafico predefinito è storicamente GNOME (anche se dopo le modifiche alla licenza delle librerie QT, KDE sta recuperando il terreno perduto). Su Internet sono disponibili le immagini ISO di tutti e 7 i CD, ma acquistandoli potrete risparmire tempo e banda, oltre che supportare attivamente il progetto.

Pro&Contro:
:) In merito ad affidabilità e stabilità, Debian non teme confronti.
:(L'installazione è piuttosto lunga e richiede spesso l'intervento diretto dell'utente; inoltre i pacchetti delle versioni stabili non sono aggiornati.

Linux Mandrake 9.0

www.mandrake.it
Versioni: Mandrake Linux 9.0 Standard (3 CD-Rom, € 35), PowerPack (7 CD-Rom € 79) o ProSuite (8 CD-Rom + 1 DVD, 395)
Kernel: 2.4.19
Facilità d'uso: *****
Completezza: ****
Sicurezza: ***

Da sempre destinata ad un pubblico meno esperto, la francese Mandrake dispone di numerosissimi tool per installazione e configurazione studiati appositamente per non gettare nel panico un utenza alle prime armi (in primis DiskDrake, per il ripartizionamente automatico dell'hard disk).
Essendo Mandrake derivata direttamente da RedHat, i pacchetti sono naturalmente distribuiti in formato RPM mentre il desktop manager principale è storicamente KDE (la distro francese nacque infatti presentandosi come una "RedHat con maggior cura per l'ambiente KDE"), anche se GNOME non è stato snobbato dagli sviluppatori.
Tra le tante, questa è nel complesso quella più adatta ad utenti alla disperata ricerca di una distro il più amichevole possibile. Su Internet ci sono le immagini ISO dei primi 3 CD

Pro&Contro:
:) La semplicità di installazione e utilizzo è per molti versi paragonabile a quella di altri sistemi operativi più diffusi.
:(I diversi tool di configurazione finiscono col nascondere molti aspetti del sistema operativo.

RedHat Linux 8.0

www.redhat.it
In vendita: Personal 7 CD-Rom, 84,70), Professional (9 CD-Rom e 1 DVD, € 302,50)
Kernel: 2.4.18
Facilità d'uso: ****
Completezza: ****
Sicurezza: ***

RedHat è forse il nome più noto nel mercato delle distribuzioni GNU/Linux; molti dei suoi dipendenti partecipano allo sviluppo del Kernel o di altri progetti Free Software quali GNOME, il formato di pacchettizzazione RPM per la distribuzione dei pacchetti è divenuto uno standard di fatto. Quest'ultima versione, sempre più orientata ad un utenza desktop, presenta strumenti di installazione e configurazione rivisti e ancora più semplificati così come l'aspetto del desktop ricorda (grazie al tema BlueCurve) quello del rivale Windows XP. Il desktop manager principale è GNOME (presente in questa distribuzione sin dal lontano RedHat Linux 6.0) e il formato predefinito dei pacchetti è, ovviamente, l'RPM.
Su Internet sono disponibili le immagini ISO dei primi 5 CD. La versione Professional include applicazioni proprietarie e il supporto anche telefonico per 60 giorni.

Pro&Contro:
:) L'installazione è decisamente semplice e con il nuovo tema Bluecurve unificato per KDE e GNOME pare quasi di lavorare sotto XP o OsX.
:(La stabilità e la sicurezza non sono hanno sempre caratterizzato le prime major release di questa distribuzione (si vedano RH 6.0 o 7.0...)

Slackware Linux 8.1

www.slackware.com
Versioni: Slackware Linux 8.1 (4 CD-Rom, $ 39,95)
Kernel: 2.4.18
Facilità d'uso: **
Completezza: ***
Sicurezza: *****

Slackware è una tra le più vecchie distribuzioni GNU/Linux e la più longeva tra quelle attualmente sviluppate. L'installazione può risultare complessa in diversi passaggi, ed avviene completamente in modalità testuale (così come testuali sono per lo più i diversi strumenti di configurazione). Atipico è anche il sistema di init, in stile BSD (anche se compatibile con il diffuso init "a-la-SysV"), o il sistema di package: sebbene RPM o DEB siano supportati, Slackware e i suoi utenti sono infatti rimasti fedeli al classico TGZ. Estremamente pulita e semplice, questa distribuzione è molto usata dai provider o, più in generale, sul lato server; un vero utente Slack perciò preferisce la shell a mille WindowManager. X è comunque ben supportato, anche se Patrick Volkerding, autore e mantainer della stessa Slackware, preferisce KDE a GNOME, ritenuto "troppo farraginoso". In generale per molti fans, Slackware incarna "Linux come è sempre stato inteso"; nel bene e nel male... Si può scaricare da Internet l'immagine ISO del CD di installazione

Pro&Contro:
:) È una tra le più sicure distribuzioni Linux esistenti, ideale per chi vuole conoscere questo SO a fondo.
:(L'installazione e la configurazione sono complicate e il sistema di gestione dei pacchetti TGZ non è tra i più comodi.

SuSE Linux 8.1

www.suse.it
Versioni: Professional (7 CD-Rom e 1 DVD, 74,90), Pro Office (in aggiunta a Suse Professional 8, 1 CD-ROM, € 24,90)
Kernel: 2.4.19
Facilità d'uso: ****
Completezza: *****
Sicurezza: ****

Tra le distribuzioni storiche, SuSe è una tra le poche distribuzioni in grado di fornire un unico pacchetto adeguato sia per il lato server che per l'ambito dekstop. YAST2, il tool grafico per l'installazione e la configurazione (inclusa una LAN Wireless) è estremamente potente e molto semplice da utilizzare mentre SaX2 permette di impostare la scheda video senza dover necessriamente intervenire manualmente sui file di configurazione. KDE 3.0 è il desktop manager predefinito e il suo aspetto, grazie anche all'utilizzo del tema Keramik e alla notevole personalizzazione operata dai grafici della casa tedesca, è decisamente piacevole. Da notare infine che, sebbene SuSE Linux sia originariamente derivata da Slackware, il formato predefinito dei pacchetti è l'RPM.
SuSE si è attirata parecchie critiche dalla comunità, perché non esiste una vera versione gratuita del sistema più recente: da Internet infatti si può scaricare solo un un live-CD dimostrativo (che non può essere installato) o un boot-CD per l'installazione tramite ftp.

Pro&Contro:
:) Accessibile ai principianti ma adatta anche ad un utenza professionale.
:(I file di configurazione vengono pesantemente "personalizzati" da YAST e SAX.

Mandrake Linux 8.2 PPC

www.linux-mandrake.com/en/ppc.php3
Versioni: Mandrake Linux 8.2 PPC (2 CD-ROM, € 29)
Kernel: 2.4.18
Facilità d'uso: *****
Completezza: **
Sicurezza: ***

Di tutte le distribuzioni provate per PPC in passato, Mandrake è stata l'unica che al primo colpo si è configurata per essere operativa su Macintosh al primo riavvio: nessun problema con la scheda grafica o con i layout della tastiera . L'unica cosa che non ha funzionato è stato l'installer in modalità grafica, ma quello a linea di comando è altrettanto semplice e funzionale. Il boot loader (Ya-Boot) permette di scegliere all'avvio se partire con Linux (tasto L), Mac OS (M), avviare dal CD-ROM (C) o passare alla schermata di selezione del sistema di avvio di Open Firmware (O, per i Mac più recenti). Anche con macchine non recentissime, quello che colpisce di più gli utenti di Mac OS X è la velocità: finestre che si aprono all'istante, pagine Web caricate e disegnate in un lampo, programmi che partono prima che possiate dire "doppio clic". Le considerazioni su KDE e Gnome sono le stesse che per la versione x86. Nonostante i due soli CD (entrambi scaricabili da Internet), c'è tutto quello che serve per un utilizzo di base, come computer personale, mentre è un po' più carente il supporto dei server.

Pro&Contro:
:) Sui Mac recenti si installa senza problemi, ed è subito pronto. Estrema velocità.
:(I software inclusi non sono tantissimi, specialmente per quanto riguarda i server (per esempio, c'è PostgreSQL ma non MySQL).

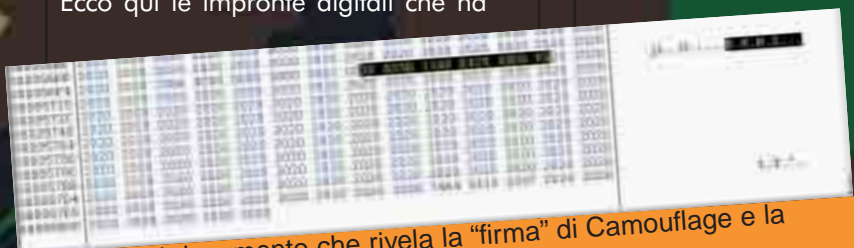
COME SCOPRIRE LE PASSWORD CHE RIVELANO I FILE NASCOSTI

TANA PER CAMOUFLAGE!

Se volete giocare a nascondino, occultando documenti importanti dentro ad altri file, state alla larga da questo programma.

Sul n. 3 di HJ avevamo parlato di Camouflage **(www.camouflagesoftware.com)**, un software per steganografia, usato cioè per nascondere un documento dentro un'altro (solitamente un'immagine). Il suo obiettivo è quindi quelllo di non far percepire in alcun modo l'esistenza di un documento nascosto. Analizzando un po' il funzionamento del programma e i file prodotti, si nota però che Camouflage non è poi così attento: **il progamma infatti "sporca" ogni file utilizzato lasciandoci sopra le sue impronte digitali**, che possono essere rese visibili con un semplice editor esadecimale.

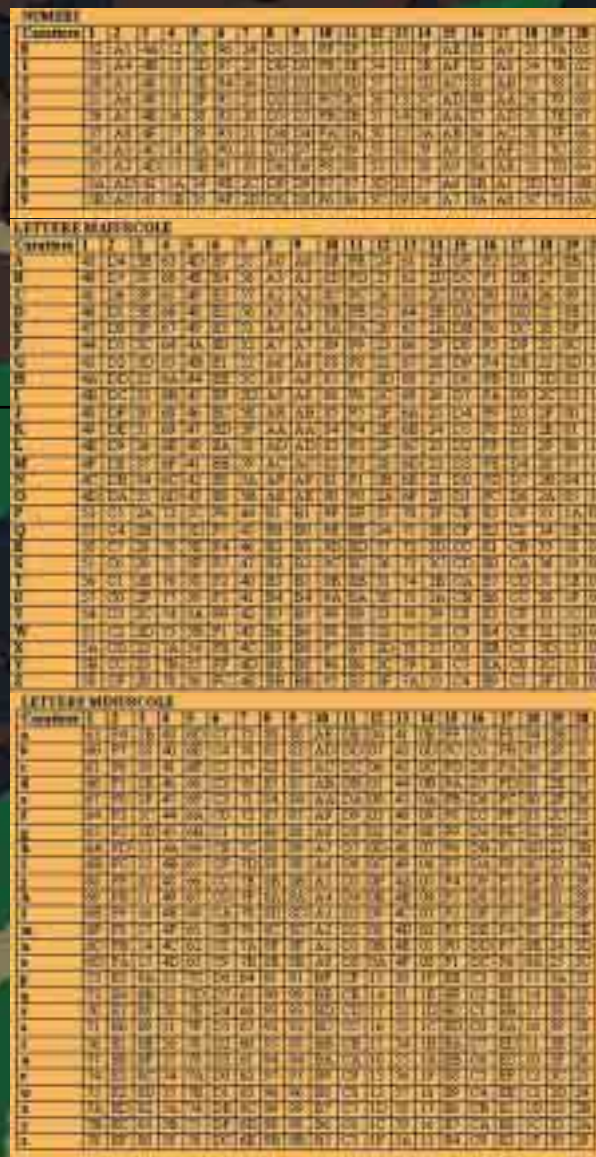
>> Tracce e indizi

Apriamo il file che sospettiamo essere stato trattato da Camouflage e precipitiamoci alla fine di tale file (vedere Figura 1). Ecco qui le impronte digitali che ha lasciato Camouflage! Alla fine di ogni file "trattato" si può riconoscere **la firma di Camouflage t.T.".** (74 A4 54 xx 22 xx).

Camouflage permette anche di cifrare il documento nascosto con una password. Anche quella può essere facilmente identificata all'interno del file, anche se cifrata. **L'ultimo carattere della password è l'ultimo carattere utile prima della firma di Camouflage** (EA in questo esempio), mentre il primo carattere della password (30 in questo esempio) è sempre quello che viene dopo i valori 00 02 00. In questo caso quindi la password è di 10 caratteri.

Una volta segnati i codici che identificano la password (30 AD 4B 13 4D E4 25 D8 D6 FA) **andiamo nelle tabelle qui a fianco e iniziamo la decifrazione!** Per esempio, andiamo a cercare il primo carattere sulla prima colonna delle tabelle; scopriamo quindi che al valore esadecimale (30) corrisponde al numero 2. Procedendo per gli altri caratteri in maniera analoga, otteniamo abbastanza rapidamente: 2811AB1975. Che è proprio la password che dobbiamo dare a Camouflage per fargli de-camuffare il file.

Oltre al fatto di "rivelare" la presenza di un file nascosto con la sua firma, Camouflage ha quindi un altro punto debole: non altera la lunghezza della password, ma si limita solamente a cifrare ogni carattere della password in un determinato modo, in base alla posizione occupata dal carattere nella password stessa.

E se quello che ci interessa è semplicemente rivelare il file nascosto, c'è persino un metodo molto più rapido: basta cancancellare la password, e Camouflage estrarrà il file senza chiedere nulla. Basta individuare la password con l'editor esadecimale, e cancellare i caratteri che la compongono (nella colonna con i valori esadecimali il valore deve essere 20).

La parte del documento che rivela la "firma" di Camouflage e la password cifrata.

>> In sintesi...

Camouflage fallisce nel tentativo di non far sapere che un file è stato camuffato e fallisce anche nel tentativo di nascondere la password. Anche se il file viene quindi cifrato in precedenza con un programma serio (come PGP/GPG), rimane il problema che un file nascosto fa scattare un campanello di allarme, e fallisce l'obiettivo della steganografia. Conviene quindi relegare Camouflage al posto che si merita, il Cestino, e **utilizzare programmi magari un po' più complicati, ma decisamente più sicuri** (una lista di tutti i programmi disponibili è su www.stegoarchive.com).

>>----Robin---->

Chi ha lasciato la porta aperta?

Credete di essere al sicuro perché non avete un server Web, ftp o telnet in esecuzione? Siete proprio sicuri che nessun'altra porta sia aperta?

Le porte di sistema sono i canali attraverso cui avviene lo scambio di dati dall'host locale verso processore verso un qualunque dispositivo di rete. Il loro numero è molto grande (65-546) e di base sono state divise in due categorie principali: le porte note e le porte non note.

Le porte note sono le prime 1024 e sono associate ai servizi di sistema; le porte non note sono tutte quelle che seguono, **dalla 1025 in poi e che sono normalmente associate a servizi non identificati**, ovvero non facenti parte del sistema stesso. Purtroppo, a parte alcuni utilizzi più che legittimi, questi "servizi" spesso si raggruppano in tre categorie: **virus, worm e cavalli di Troia.**

I virus sono dei programmi che si autoreplicano e si diffondono usando altre applicazioni all'interno del PC ospite.

I worm funzionano come i virus con la differenza che si propagano attraverso la rete.

I cavalli di Troia sono applicazioni che mascherano, sotto l'apparenza di un programma utile, un codice dannoso che può svolgere svariate attività all'interno del PC.

>> Diamo i numeri

Vediamo ora nel dettaglio le più "note" fra le porte non note e i pericoli che possono rappresentare. Come noterete, all'inizio dell'elenco vi sono anche alcune porte inferiori alla 1024 (porte note), che però possono essere usate in modo fraudolento da programmi diversi da quelli per cui sono state pensate e riservate.

Porta 21, 5400
Programmi come Blade Runner, FTP trojan, Invisibile FTP, WinCrash utilizzano la porta 21 per creare varianti pericolose del servizio FTP; queste varianti possono essere controllate in remoto e permettono l'upload o il download di file e programmi.

Porta 23
È talvolta sfruttata dal servizio TTS, che funziona come un programma di emulazione terminale che opera in maniera invisibile (un server telnet nascosto). Una volta connessi in modalità telnet classica si riescono a impartire comandi da eseguire sul sistema colpito.

Porta 25, 110
Molte applicazioni a prima vista innocue che simulano fuochi d'artificio o l'esplodere di un tappo di spumante, nascondono demoni in grado di rubare password di sistema e di spedirle via email. Se non state usando programmi per la posta, ma vedete aperte queste porte, c'è qualcosa che non quadra.

Porta 31, 456, 3129, 40421
Servizi come Hackers Paradise usano soprattutto la porta 31 per acquisire il controllo del sistema e per modificare il registro di configurazione.

Porta 41, 2140, 3150, 60000
Un daemon noto col nome di Deep Throat offe enormi possibilità di gestione remota del PC, fra le quali: server FTP, amministrazione remota, cattura schermo, gestione dei processi in esecuzione.

Porta 113
Il servizio Kazimas è un worm che si autodiffonde attraverso mIRC. Una volta infettata la macchina, si autoreplica e cambia il file di impostazioni del mIRC stesso.

Porta 119
Il famosissimo Happy 99 ad una prima occhiata sembra un innocuo passatempo tutto pieno di fuochi d'artificio, ma in verità nasconde un pericolosissimo programma di prelevamento password, mail spamming ed attacchi DoS.

Porta 555, 9989
Programmi come NeTAdmin e Stealth Spy hanno come scopo quello di distruggere il sistema infettato dopo essersi riprodotti e distribuiti.

Porta 1010, 1015
Il servizio noto come Doly Trojan è un

cavallo di Troia capace di acquisire completamente il controllo remoto del PC infettato.

Porta 1024, 31338
Il servizio NetSpy è uno dei più noti in grado di spiare l'attività all'interno di un PC e di gestirla in remoto. Può anche bloccare il pulsante start e nascondere la barra delle applicazioni.

Porta 1234
Il daemon Ultors è un altro trojan in grado di far acquisire il controllo remoto della macchina infettata.

Porta 1600
È associata a un trojan di concezione molto semplice, il Shivka-Burka, che ha solo funzionalità di trasferimento files.

Porta 1999
Il servizio BackDoor è stato uno fra i primi cavalli di troia con associata una backdoor. Offre svariate possibilità di controllo remoto del PC come controllo del mouse, video, task, chat e messaggistica.

Porta 2115
Bugs è un programma di accesso remoto che consente la gestione dei file e l'esecuzione di comandi.

Porta 2155, 5512
Il daemon Illusion Mailer è un programma di spamming di posta elettronica che consente di inviare messaggi usufruendo dell'identità della vittima.

Porta 2565
Il servizio Striker, associato a questa porta, ha come unico intento quello di far fuori Windows. Dopo il riavvio comunque non rimane residente in memoria e pertanto se l'attacco viene evitato, non si corrono rischi futuri.

Porta 2583, 3024, 4092, 5742
Un cavallo di troia noto col nome di WinCrash sfrutta queste porte per insediarsi e per compiere la sua azione. Essendo dotato di strumenti come il flooding, è considerato uno strumento potente e pericoloso.

Porta 2600
Il daemon RootBeer è un cavallo di Troia dotato di accesso remoto con le seguenti caratteristiche: messaggistica, controllo finestre, controllo monitor, controllo audio, controllo modem, congelamento del sistema.

Porta 2989
Il servizio RAT è un cavallo di Troia a backdoor progettato per distruggere il contenuto dei dischi rigidi di sistema.

Porta 3459, 3801
Il daemon Eclipse è un servizio FTP invisibile che dà accesso al trasferimento dei file ed alla loro esecuzione, cancellazione e modificazione.

Porta 4567
Il servizio File Nail è una backdoor remota associata ad ICQ.

Porta 5001, 30303, 50505
Il virus Sockets de Troie è un programma che si diffonde come una backdoor di amministrazione remota. La sua istallazione coincide con un errore DLL e, dopo essersi istallato nella directory \windows\system, modifica le chiavi del registro di configurazione.

Porta 6400
Il daemon tHing ha la sua pericolosità non tanto nella sua attività intrinseca, ma perché viene sfruttato da virus come metodo di infezione di altre macchine.

Porta 7000
I daemon Remote Grab è in grado di catturare schermate del monitor remoto, in modo tale da avere una visione esatte delle attività svolte.

Porta 10101
Il cavallo di Troia BrianSpy è dotato di tutte le classiche funzionalità di questi programmi, con l'aggiunta di un servizio grazie al quale riesce a eliminare i file di scansione degli antivirus istallati.

Porta 12223
Il servizio che sfrutta questa porta è un KeyLogger che ha la possibilità di inviare in tempo reale al cracker tutta l'attività svolta sulla tastiera del PC remoto.

Porta 12345
Forse la più nota tra le porte non note: è la porta a cui risponde il server della backdoor NetBus, ormai vecchiotta ma ancora in grado di creare danni.

Porta 20000
Il trojan Millennium è un programma scritto in VB che offre come caratteristiche: controllo file, controllo CD-ROM, controllo barra applicazioni, controllo audio, prelievo password, controllo browser, riavvio del sistema.

Porta 22222, 33333
Il cavallo di Troia Prosiak è l'ennesimo daemon di controllo remoto che offre il classico arsenale di funzioni tipiche di questa categoria di programmi.

Porta 31337, 54320
Il daemon Back Orifice è un programma altamente pericoloso che sta alla base della concezione di sviluppo di altri Trojan per Windows.

La prudenza non è mai troppa

Come è facile immaginare la possibilità da parte di un cracker di avere libero accesso alle porte è di vitale importanza per compiere la sua opera distruttiva. Questo lunghissimo elenco di porte e di servizi associati deve servire come stimolo all'autoprotezione. Un buon firewall, pur magari non essendo la soluzione a tutti i mali, impostato nei limiti del possibile con delle regole abbastanza ferree sulla possibilità di utilizzare determinate porte, può certamente limitare le strategie di ingresso nel PC da parte di estranei. Se ad asso infine associamo anche una scansione periodica con antivirus ed una scansione del proprio sistema a caccia di "porte aperte", probabilmente potremmo riuscire ad avere una fotografia sufficientemente esaustiva della nostra sicurezza, mettendoci così nella possibilità di correre ai ripari chiudendo le varie falle sul nostro PC.

CAT4R4TTA
cat4r4tta@hackerjournal.it

COME INDIVIDUARE PROGRAMMI MALIZIOSI NEL PROPRIO PC

CLANDESTINI A BORDO

Programmi come i cavalli di Troia e i keylogger solitamente si nascondono nel sistema infettato, e non vengono rilevati facilmente dalle utility più comuni: ecco come scovarli.

Come abbiamo già visto nei numeri scorsi, i Keylogger possono rivelarsi dei potenti strumenti a disposizione di cracker e lamer di ogni sorta, visto che sono molto semplici da installare e configurare.
È quindi indispensabile **comprenderne i meccanismi di funzionamento per identificarne l'eventuale presenza e procedere a una disinstallazione**.
Nei sistemi operativi più semplici come le versioni di Windows che arrivano fino alla Millennium, per i programmatori è sempre stato facile occultare (almeno agli occhi della maggioranza degli utenti) la presenza di processi presenti in memoria con dei semplicissimi accorgimenti.
Un esempio potrebbe essere, utilizzando un qualsiasi linguaggio di programmazione, il seguente codice:

```
RegisterServiceProcess(GetCurrentProcessId()
, 1);
```

In questo modo, l'utente che provasse a ottenere la lista dei processi attivi con il Task Manager (Ctrl+Alt+Canc), non vedrebbe il processo "nascosto" nella lista che mostra tutti i programmi aperti. Una soluzione a tale inconveniente potrebbe essere l'adozione di un programma apposito e più avanzato rispetto alla task list standard, come per esempio AVP System Watcher disponibile qui all'indirizzo www.avp.it/future.htm
Meglio ancora, conviene fare affidamento su sistemi operativi più robusti come NT/2000/XP, che almeno queste rudimentali tecniche di mascheramento le bloccano già di default.

>> Funzionalità di Keylogger e Backdoor

Una volta che una backdoor viene installata in un computer, ha bisogno necessariamente di attivarsi ogni volta che l'utente accende il proprio PC. Per ottenere il suo scopo, **deve obbligatoriamente posizionarsi in uno di quei file che vengono letti al momento del boot** e che sono WIN.INI e SYSTEM.INI oltre che nel Registro di Windows. Di quest'ultimo, in particolare, bisogna tenere d'occhio alcune chiavi critiche:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current
Version\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current
Version\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current
Version\RunOnceEx
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current
Version\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current
Version\RunServicesOnce
```

Queste sono infatti le chiavi più utilizzate dalle backdoor che si trovano in rete, anche se bisogna fare attenzione anche a tutte le operazioni che quotidianamente vengono compiute dagli utenti, come l'esecuzione di programmi e l'apertura di documenti html:

```
HKEY_CLASSES_ROOT\exefile\shell\open\command
```

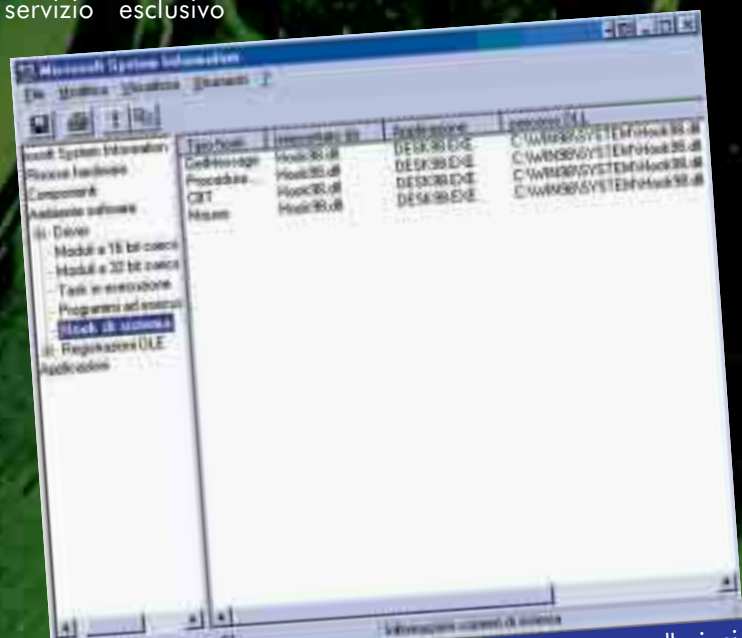
dove il valore non alterato dovrebbe essere simile a questo:

"%1 %*"

```
HKEY_CLASSES_ROOT\htmlfile\shell\open\com-
mand
```

con valore simile a:

```
"C:\PROGRA~1\INTERN~1\iexplore.exe" -nohome
```

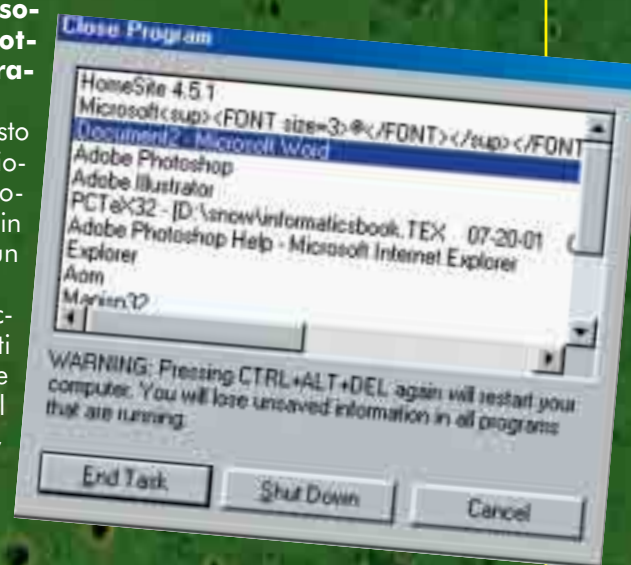
Al posto del valore %1 potrebbe esserci infatti il percorso di una backdoor, che così verrà attivata a ogni esecuzione del programma.
Queste sono le tecniche principali per far partire all'avvio un programma di spionaggio, anche se possono esserci delle variazioni sul tema come l'utilizzo del comando AT, che è un servizio esclusivo dei sistemi NT/2000/XP e che permette la pianificazione di operazioni ad intervalli di tempo.

L'utility msinfo32, presente nella maggior parte delle installazioni di Windows, permette di visualizzare gli hook di sistema, e accorgersi quindi di eventuali keylogger.

>> Registrare le operazioni con la tastiera

A oggi, i più moderni keylogger offrono numerose funzionalità aggiuntive come la cattura dello schermo, di immagini da una webcam installata eccetera, ma il loro compito principale resta sempre uno: quello di registrare l'attività della tastiera.
Per far ciò, Windows mette a disposizione il meccanismo dello hooking, che consiste nel permettere ad un programma di **intercettare gli eventi del sistema (come appunto la digitazione) e di registrarli in un determinato file**.
Tale meccanismo è però in parte controproducente nel mascheramento dell'applicativo, visto che per effettuare tale funzione di hooking un programma deve necessariamente collocare la propria parte di codice relativa alla 'cattura' dei tasti in una libreria .DLL caricata nello spazio di memoria del SO.
Queste librerie necessarie all'hooking **sono facilmente intercettabili con un'utility già presente in molte versioni di Windows** (ma non in tutte!) che è Msinfo32. Questo programma ha infatti una voce specifica per visualizzare gli Hook di sistema.
Bisogna ricordare che **gli hook di sistema non sono sempre delle applicazioni di backdoor o dei keylogger**; infatti, molti driver per i mouse o per le tastiere sfruttano tale meccanismo per poter offrire dei servizi aggiuntivi agli utenti, e quindi bisogna prestare attenzione ad eventuali falsi allarmi.
Un altro meccanismo, finora non utilizzato da alcun keylogger ma dalle molte potenzialità, è quello della lettura della coda dei messaggi della tastiera.
Tale metodo sfrutta una API a livello utente che è GetAsyncKeystate e permettere di leggere ogni tasto digitato dall'utente, qualunque applicativo esso stia utilizzando.
La differenza sostanziale risiede nel carico computazionale della chiamata a tale funzione, che deve essere effettuata in maniera ciclica (polling) e quindi tende a consumare risorse di Cpu, anche se in modo non poi così eccessivo. Il vantaggio consiste però nel fatto che non installando degli hook di sistema, non viene elencata dall'utility msinfo32 risultando dunque più difficile da individuare.

>> Come difendersi?

Ci si può a questo punto chiedere se sia possibile essere infetti da una backdoor completamente invisibile magari progettata da qualche governo o peggio ancora da qualche nostro rivale. La risposta che mi sento di dare in tutta tranquillità è negativa. Ci possono essere infatti delle backdoor progettate con estrema cura, ma **nessun programma (a meno di utilizzare un LKM) può essere così sofisticato da sottrarsi all'enumerazione del SO**.

La risposta è presto data, per la maggioranza di tali programmi circolanti in rete: utilizzare un personal firewall.
A parte i vari attacchi portati avanti contro tali software i personal firewall sono molto sicuri, anche se ci sono a volte delle eccezioni con alcune backdoor.
Il problema viene infatti dalle cosiddette Shell Extensions che sono delle funzionalità messe a disposizione dei programmatori ed in grado di 'estendere' il SO. Tali librerie possono essere utilizzate per **ingannare i firewall e far credere che sia il SO a volersi connettere ad Internet, mentre è invece il Keylogger**.
Un esempio di tale programma è Spector, che sfruttando tale meccanismo viene visto dal firewall come il processo explorer.exe, mentre in realtà non è altro che tale programma a voler superare il meccanismo di filtraggio del firewall. Occhio quindi al software presente sui vostri PC.

Paolo Iorio
www.paoloiorio.it

CHIUDERE ALCUNI BUCHI NEL MODEM ALCATEL SPEED TOUCH

UN MODEM PERICOLOSO

Un malintenzionato potrebbe prendere il totale controllo di un diffuso router Adsl di Alcatel

Il modem in questione è un router DSL molto diffuso, soprattutto fra l'utenza italiana, dato che molti ISP lo distribuiscono in comodato insieme all'abbonamento. È sicuramente un prodotto affidabile, di facile installazione, configurazione e impostazione dei parametri, grazie al suo menu molto intuitivo e a un help che istruisce su tutte le più importanti funzioni.

Ha solo un piccolissimo ed insignificante "problemino"… Se una volta istallato non si aggiorna il firmware, un qualunque malintenzionato può accedervi in circa 5 secondi!

Già alla fine del 2000, ricercatori dell'Università di California (bei tempi quando, pur studiando tutt'altro, ci vivevo anche io…) avevano identificato alcuni difetti che permettevano, se sfruttati in maniera adeguata, di prendere il completo controllo del dispositivo, cambiare le sue impostazioni, cambiare la password ed uploadare il firmware aggiornato, cosicché il legittimo proprietario non potesse poi a sua volta recuperarlo usando la stessa tecnica di scassinamento.

Più nello specifico, i "difetti" permettono di:
* Cambiare la configurazione del dispositivo in modo tale che non possa più essere accessibile.
* Disabilitare temporaneamente o permanentemente il router.
* Installare determinati script tipo sniffers di traffico o tools DoS.

Tutto ciò è possibile grazie a un particolare sistema di decifratura di un codice restituito dal router, che permette di bypassare qualunque password impostata dall'utente.

L'help del comando Nat fornisce tutte le operazioni eseguibili nelle tabelle di routing.

Inserendo un determinato username si ottiene un output del tipo SpeedTouch (xx-xx-xx-xx-xx-xx) che se interpretato tramite un sistema di decodifica dà la password da inserire per accedere al dispositivo. Subito sotto infatti si nota la schermata di benvenuto del router.

>> I bug del sistema

Nel momento in cui ricevete il router non c'è nessuna password impostata all'interno. Sembrerà assurdo ma una grandissima percentuale di utenti non compie questa semplicissima operazione e un giorno, andando a settare il router, non riesce più ad entrare al suo interno…il motivo?? Beh…se voi vi scordate di settare la password forse qualcuno se ne ricorderà al posto vostro… Del resto accedere al router è molto semplice dato che oltre via telnet si può configurare anche via http collegandosi ad esso con un normalissimo browser, mentre i files contenuti all'interno possono essere analizzati via FTP.

Le password possono essere facilmente rubate: il router è aperto a connessioni non protette di tipo TFTP. Il file delle password può essere facilmente scaricato e decifrato con calma.

By-pass delle password di sistema

Come detto in precedenza, alla richiesta di connessione via telnet/http, il router domanda username e password. Se inseriamo un username ben preciso riceviamo un output del tipo "SpeedTouch (xx-xx-xx-xx-xx-xx)"; questa stringa può essere decrittografata in maniera molto semplice. L'output che riceviamo sarà di norma un numero di 8-10 cifre che, usato come password, dà l'accesso al router. Esiste un solo metodo per ovviare a questo inconveniente, ovvero

Modelli e versioni a rischio

I modelli interessati sono sicuramente gli Speed Touch Home e gli A1000, anche se molto probabilmente anche i Pro potrebbero essere affetti da questi bugs essendo essi stessi basati su un codice molto simile.

Le versioni di firmware sicuramente incriminate sono le seguenti:

KHDSAA.108 6 Luglio 1999
KHDSAA.132 19 Novembre 1999
KHDSAA.133 16 Marzo 2000
KHDSAA.134 24 Aprile 2000

aggiornare il prima possibile il firmware del dispositivo.

Connessioni TFTP
Il servizio TFTP è facilmente accessibile dall'interno della rete, ma anche dall'esterno. Senza nemmeno studiare troppo, si riesce facilmente a usufruirne. Nel momento dell'imballaggio, il router è configurato per avere sempre aperta una porta TFTP che può essere utilizzata sia per trasferire che per

```
=>help
Following command groups are available
                                   softwar
config        system               ppp
nat           cip
```

Tramite il comando help possiamo ricevere una lista di funzioni utilizzabili; le più interessanti per un crakkatore sono di certo il config da cui impostare la password ed il nat da cui impostare gli ip di routing.

prelevare file dall'interno. Tale porta risponde sempre a pacchetti provenienti da IP tipo 255.255.255.255 e ciò predispone una possibilità di attacco utilizzando una porta ECHO UDP. Quando il server ECHO risponde alla richiesta, esso interpreta l'indirizzo di destinazione 255.255.255.255 come facente parte del broadcast locale, e il pacchetto viene spedito nella Ethernet con la porta associata all'UDP TFTP. Questo bug può essere sfruttato per catturare i file di configurazione e di archiviazione delle password. Inoltre si può utilizzare per l'upload di script tipo sniffers di traffico. Ovviamente essendo una connessione non protetta, non necessita nemmeno di username o password.

Nella tabella di routing si vede la configurazione della rete. Se notate bene al punto 9 c'è un reindirizzamento esterno…potrebbe essere un accesso a qualche server?? (NB. Parte degli indirizzi IP sono stati volutamente coperti).

Inadeguata validazione dei firmware
I supporti Alcatel sembra che non svolgano alcun test di integrità dei firmware caricati, così chiunque può creare un suo firmware, patchato con script nocivi tipo sniffer o tools DoS, e uploadarlo all'interno del router, sfruttandolo quindi per attività illecite.

L'EXPERT mode
Lo Speed Touch ha un expert mode che può essere utilizzato per scoprire informazioni interessanti sul router e sulla configurazione della rete, nonché per impostare un'infinita varietà di parametri del device stesso. La "particolarità" di questa modalità risiede nel fatto che anch'essa basa la sua password di accesso sullo stesso sistema di crittografia.

>> Oltre al danno la beffa

Rilasciare un prodotto con così tante falle di sicurezza è già abbastanza grave. Ma Alcatel sembra addirittura peggiorare la situazione con le informazioni contenute nel suo sito. Tra le Faq, infatti, vi è una domanda relativa alla sicurezza del router. Ebbene, a chi chiede se l'assenza di un firewall renda l'A1000 poco sicuro, Alcatel risponde che con le impostazioni standard non consentono alcuna connessione dall'esterno, a meno che non sia stata richiesta dalla propria macchina. Dopo quello che abbiamo visto finora, questa rassicurazione non può fare altro che farci sorridere (o preoccupare, se si possiede un router di questo tipo e non si è provveduto all'aggiornamento del firmware…).
Al momento attuale l'unico sito consultabile per l'aggiornamento è

Ci si può collegare al sistema di configurazione del router anche tramite web. Ecco la schermata iniziale.

Welcome to the World of ADSL

E si può anche configurare la tabella di routing…

http://security.sdsc.edu/self-help/alcatel/tools dove peraltro si trova un firmware che comunque deve essere utilizzato con cautela. Vi consiglio di conseguenza di crearvi prima una copia del firmware esistente e poi passare all'upgrade. Per effettuarlo la procedura più intuitiva consiste nel collegarsi via web al proprio router, cliccare sul pulsante upgrade e cancellare la versione passiva del software. Effettuati questi passaggi il nuovo file deve essere uploadato e poi switchato come versione attiva. Se tutto procede correttamente in meno di cinque minuti avrete il vostro router aggiornato e protetto contro "curiosi invadenti".

CAT4R4TTA,
cat4r4tta@hackerjournal.it

N.B. Sono stati volontariamente evitati riferimenti diretti a username e password standard, nonché a siti dove si possano trovare tools di decifrazione delle password.

DIFESA E CONTRATTACCO

Un firewall gratuito per uso personale ma efficace e con molte funzionalità che mancano in tanti suoi concorrenti.

FUNZIONALITÀ E CONFIGURAZIONE DI SYGATE PERSONAL FIREWALL

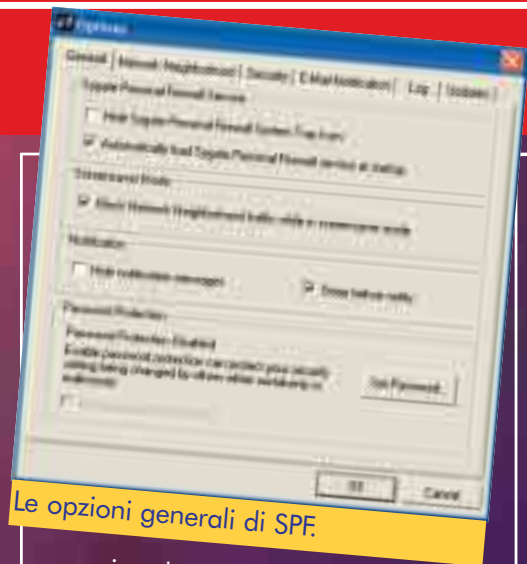
Purtroppo, al giorno d'oggi nessuno può permettersi il lusso di rimanere collegato a Internet senza un buon firewall. Per fortuna la ricerca a programmi volti a difenderci dai sempre più frequenti AdWare, SpyWare, troyan e da tutti quei sistemi che possono mettere in pericolo non solo la nostra privacy ma anche la sicurezza dei dati, sembra aver portato alla creazione di **firewall efficienti, molti dei quali gratuiti per l'uso personale**. Uno di questi, certificato dai laboratori dell'ICSA (una delle maggiori istituzioni nella certificazione di sistemi per la sicurezza) è Sygate Personal Firewall (SPF), giunto alla versione 5, prodotto dalla Sygate e scaricabile dal sito (www.sygate.com), dove è inoltre possibile trovare anche una versione "Pro" dello stesso, dotata di funzioni aggiuntive ma rivolte per lo più all'attenzione d'aziende.

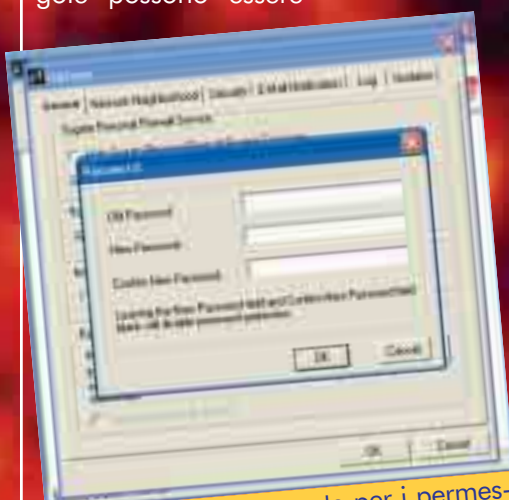
>> Primi passi

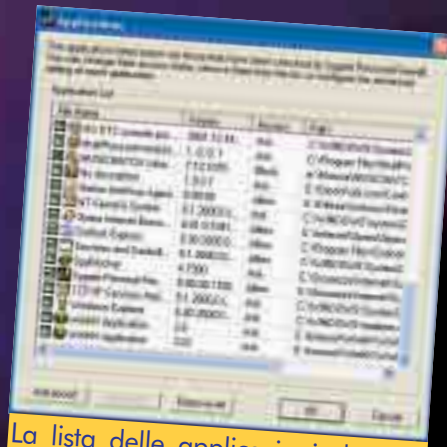
Vediamo ora, più in dettaglio, quali sono le principali funzioni e le potenzialità di SPF. Innanzi tutto occorre scaricare il firewall, circa 5 Mb, e installarlo. Questa procedura è al solito guidata nei suoi passi e non dovrebbe presentare problemi. Successivamente sarà necessario riavviare il computer.
Terminate queste prime operazioni, il programma si caricherà a ogni avvio di Windows, inserendo un'apposita icona nella barra delle applicazioni (utilizzabile anche per accedere ai menu). Nel caso si volesse disattivare questa opzione, basterà disabilitare la voce "Load Sygate Personal Firewall service at startup" nel menu Tools/Options/General/Automatically.
A questo punto, una volta connessi a Internet, **sarà abbastanza comune per le prime volte vedere comparire finestre pop- up ogni qual volta un programma tenta di accedere alla rete**. Questi messaggi, oltre a notificarci i tentativi di connessione segnalandoci l'indirizzo ip a cui ci si sta per collegare (ed altre informazioni di carattere più tecnico fornite premendo il pulsante Detail), richiedono anche di impostare le prime semplici regole per permettere le connessioni di quello specifico programma (queste impostazioni saranno comunque modificabili in seguito).
Facendo invece doppio clic sull'icona di SPF nella barra delle applicazioni, apparirà l'interfaccia principale del programma. Questa mostra, con un aiuto grafico, le informazioni d'immediato interesse, come per esempio una lista delle applicazioni attive e connesse alla rete, o il resoconto sul traffico di dati in ingresso ed in uscita, con le relative eventuali porzioni bloccate.

La finestra principale del programma.

>> Configurazione

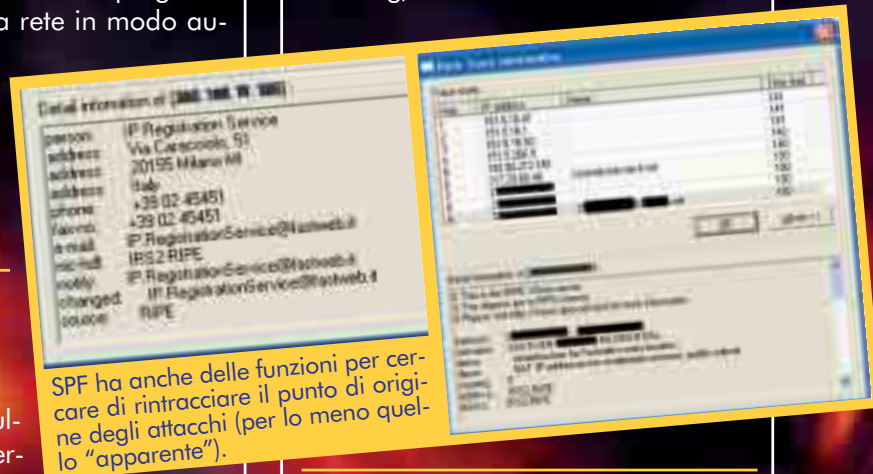
Accedendo al menu delle opzioni (Tools/Options oppure con il pulsante destro sull'icona SPF) sarà invece possibile scorrere attraverso diverse finestre, che permettono una più approfondita analisi e modifica delle impostazioni.
Le principali tra queste sono:
possibilità di bloccare le impostazioni del firewall, compreso l'avvio o la chiusura del programma, tramite password;
- condivisione, a livello lan, di file e stampanti;
- notifica automatica tramite mail di un eventuale attacco subito dal sistema;
- verifica, sempre in automatico, di nuove versioni del SPF più aggiornate;
- modifica delle dimensioni dei ffiledi log a livello di "security", "system", "traffic" e "packet" (questi file sono una sorta di scatola nera del sistema con-

Le opzioni generali di SPF.

nesso in rete, lo vedremo avanti).
Sempre dall'interfaccia principale sarà inoltre possibile visualizzare, tramite il pulsante "Applications" un riquadro contenente **l'intera lista di tutti quei programmi che abbiano cercato, almeno una volta, di connettersi in rete**. A sinistra del nome dell'applicativo verrà indicata la regola di "policy" vigente (accetta, chiedi o rifiuta), modificabile semplicemente cliccandoci sopra.
Selezionando da questa lista un programma, e cliccando sul pulsante "Advanced", situato in basso, si aprirà invece un menu d'opzioni avanzate che consentiranno di impostare delle restrizioni sugli IP o sulle porte considerate sicure.
Questa finestra di configurazione, come quella per la creazione di regole avanzate ("tools/advanced rules"), richiederebbero un minimo di conoscenze tecniche da parte dell'utente. Le regole possono essere

Le impostazioni avanzate per i permessi attribuiti a un programma.

applicate a una specifica interfaccia di rete o a tutte, a un singolo indirizzo IP, a una sottorete intera tramite l'utilizzo di una netmask, oppure si può applicare la regola a una macchina precisa tramite Mac Address (l'indirizzo fisico dell'interfaccia di rete).
Sara inoltre possibile configurare tutte quelle impostazioni di "scheduling", ovvero **l'apertura e la chiusura sincronizzata di una determinata porta verso un determinato IP in**

La lista delle applicazioni che, almeno una volta, hanno tentato un collegamento in rete.

momenti particolari, impostati dall'utente e che permettono al programma di accedere alla rete in modo automatico, senza lasciare potenziali falle nel sistema una volta che questi compiti sono terminati.

Attacco e risposta

Passiamo ora al pulsate LLogs dell'interfacciaprincipale: questa finestra racchiude tutte le informazioni sulle attività del firewall e della connessione in rete, informazioni che si possono esportare a piacimento in diversi formati. Si divide in Security, Traffic, Packet e System.
Quella più interessante è forse Security log, poiché è quella che ci fornisce **tutte le informazioni relative agli attacchi recenti e passati subiti dal nostro computer**. Ma non solo. È anche quella che ci permette di compiere una sorta di risposta a questi tentativi d'intrusione più o meno maliziosi. Quando infatti subiamo un tentativo d'attacco, l'icona di SPF nella barra delle applicazioni comincerà a lampeggiare, segnalandoci inoltre l'evento con un messaggio poco sopra questa.
Cliccando sull'icona apparirà la finestra Security log con tutte le informazioni del caso, suddivise anche per grado di pericolosità. Selezionando l'attacco appena subìto, in modo da evidenziare l'intera riga, e premendo il pulsante Back Trace (in Action/back trace), **SPF sarà in grado di risalire il percorso compiuto dal tentativo d'aggressione dal nostro computer fino alla sorgente**.
Questa si rivelerà essere quasi sempre non il PC attaccante, ma il router pubblico usato per compiere l'azione. A questo punto, per avere informazioni relative al possessore del router, bisogna premere su Whois, un pulsante situato in fondo alla finestra delle informazioni di Back trace.
Ora non rimarrà altro che contattare, tramite mail o altro, il possessore del router, fornendogli tutte le informazioni relative all'attacco esportando il nostro file di log, anche in formato txt.

SPF ha anche delle funzioni per cercare di rintracciare il punto di origine degli attacchi (per lo meno quello "apparente").

Servizi aggiuntivi

L'interfaccia principale fornisce anche altri servizi aggiuntivi, individuabili attraverso i pulsanti Test e Help. Entrambi conducono al sito della Sygate e consentono di **compiere una verifica, attraverso varie scansioni e simulazioni d'intrusione, sull'efficienza delle nostre difese e sulla sicurezza del sistema** (scan). Il tasto Help invece, com'è facile intuire, porta alla pagina internet da dove si può accedere al manuale in linea, situato comunque anche nella cartella d'installazione di SPF.

Fabio Mingotto

IDENTIFICATION
ORDER NO. 13
November 21th, 2002

WANTED

DIVISION OF INVESTIGATION
H.J. DEPARTMENT OF NET
CERNUSCO S.N., MI

Fingerprint Classification

16 0 5 U 001 20
1 17 U 001

NAME: Nimda
TYPE: Worm
DATA DI NASCITA: 18 Settembre 2001
ALIES: W32/Nimda@mm, PE_NIMDA.A, I-Worm.Nimda, W32/Nimda-A, Win32.Nimda.A
DIMENSIONI dell'infezione: 57.344 byte
SISTEMI A RISCHIO: Tutte le versioni di Windows; sono immuni all'infezione Macintosh e Unix

Nello scorso numero abbiamo parlato dei numerosi pericoli che si corrono in rete e accennammo ai worm che sono attualmente in circolazione dato che sono riusciti a diffondersi maggiormente tra i sistemi provocando non pochi danni. Un worm che merita un po' più di attenzione rispetto agli altri è il Nimda, scoperto il 18 Settembre 2001 che provoca molti danni e presenta un alto rischio di riceverlo. Il suo punto di forza è che, per rimanere infettati da Nimda, è sufficiente visitare un sito infetto perché subito venga richiesto il download di un file .eml. Si può ricevere l'infezione anche con una semplice anteprima di un messaggio email che lo contiene. Il nome del worm deriva dalla lettura al contrario della parola "admin". Il worm si diffonde per email, attraverso i network aperti, provvede a copiarsi nei server web Microsoft più vulnerabili non protetti ed è un virus che infetta sia i file locali sia quelli condivisi sui network remoti.

Modalità di contagio

Quando il worm arriva per email, usa un exploit MIME che gli permette di eseguirsi semplicemente con una lettura o un'anteprima dell'email che lo contiene come allegato. Le più recenti versioni di Microsoft Outlook e Outlook Express sono immuni da questo baco; se è stato eseguito l'aggiornamento, si può quindi stare relativamente tranquilli. Se si visita un server web infetto, si potrebbe ricevere tramite il download un file .eml (un messaggio di posta elettronica in formato Outlook Express) che contiene l'infezione. Per rimediare a questo rischio, si può disabilitare il Download Automatico del proprio browser nelle opzioni. Per di più, il worm crea un network aperto sul computer infetto, che permette l'accesso al sistema a utenti non autorizzati.

Nimda contiene inoltre una routine di mass-mailing, che viene eseguita ogni 10 giorni. Il worm inizia questo processo cercando gli indirizzi email nei file .htm e .html presenti nel sistema infetto; questi indirizzi vengono usati per riempire i campi del mittente e del destinatario in modo che, quando le email saranno ricevute, sembrerà che siano state inviate da altre persone, il cui indirizzo era presente sul computer infetto. Il worm usa un proprio server SMTP per inviare le email infette che contengono un file di nome Readme.exe di 57344byte (che potrebbe non essere visibile come allegato nell'email ricevuta).

Operazioni compiute

Nimda modifica alcuni file sovrascrivendoli con l'infezione, causa dei rallentamenti al sistema (potrebbe essere un sintomo per individuare un computer infetto) e apre l'unità C come un network di file sharing. Il worm provvede a infettare i file .EXE ma prima di farlo controlla se il file è stato già infettato precedentemente dal virus. Se il file risulta essere non infetto, il worm provvede a copiare se stesso nella cartella dei File Temporanei; il file EXE in questione viene inglobato in questa copia. Questo nuovo file viene poi sostituito al file originale con il risultato del file originale con l'infezione aggiunta. Quando un file infetto viene eseguito, il worm estrae il file originale temporaneamente e lo esegue insieme all'infezione; in questo caso non si sarà avvertiti che quegli eseguibili contengono l'infezione.

Durante l'esecuzione, il worm potrebbe anche cancellare le copie di se stesso ma se il file è in uso o bloccato, il worm è in grado di creare il file Wininit.ini con una stringa che provvede a cancellare il worm al primo riavvio del sistema. Mentre infetta i file eseguibili, il worm potrebbe creare due file infetti nella cartella dei File Temporanei di Windows che saranno nascosti e avranno gli attributi di file di sistema.

Dettagli tecnici

Nimda infetta i server web Microsoft IIS non protetti e su Microsoft IIS 4.0 e 5.0 è possibile che crei un URL che trasmetta l'infezione ai visitatori.

Per quanto riguarda le modifiche al sistema, quando il worm viene eseguito sovrascrive il file Mmc.exe nella cartella Windows oppure crea una copia di se stesso nella cartella dei File Temporanei. Il worm procede infettando i file eseguibili (escluso il fileWinzip32.exe) e copiando l'infezione in file .eml, .nws (creati dal worm e non presenti già nel

sistema) nelle cartelle che contengono file .doc; inoltre il worm crea alcuni file nel sistema e nelle chiavi di registro:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\App Paths
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Explorer\Shell Folders
```

Il worm infetta il sistema modificando anche il file System.ini nel modo seguente:

```
Shell = explorer.exe load.exe -dontrunold
```

Inoltre sostituisce il file Riched20.dll, usato da programmi come Microsoft Word, in modo che il worm sia eseguito ogni volta che si avvia un programma che sfrutta questo file (come appunto Word).
Il worm copia se stesso anche come il file load.exe nella cartella C:\Windows\System\ e crea dei netword di file sharing aperti modificando la chiave del registro

Nimda usa quattro differenti canali di infezione: le email, i server Web, le reti locali e i file .exe.

```
HKLM\Software\Microsoft\Windows\
CurrentVersion\Network\LanMan\[C$ -> Z$]
```

(E' necessario un riavvio del computer per rendere effettive le impostazione modificate dal worm)
Le porte utilizzate da questo worm sono elencate di seguito. Bisogna fare attenzione al fatto che si tratta di porte standard, che potrebbero quindi essere confuse con servizi leciti:

TCP 25 (SMTP) - usata per inviare email infette agli indirizzi trovati sul PC della vittima
TCP 69 (TFTP) - apre la porta 69/udp per il trasferimento TFTP di admin.dll e per le connessioni in uscita per il trasferimento dei file
TCP 80 (HTTP) - usa questa porta per colpire i server più vulnerabili
TCP 137-139,445 (NETBIOS) - usata per la trasmissione del worm

In aggiunta il worm controlla le connessioni che trasferiscono una particolare sequenza di byte e poi apre una porta specifica nella richiesta di connessione.

Come difendersi e rimuoverlo

Symantec ha prontamente realizzato e messo a disposizione un software per rimuovere l'infezione causata da Nimda che potete scaricare all'indirizzo http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.removal.tool.html

Una volta che il computer è stato attaccato e infettato da Nimda, è possibile che un utente non autorizzato abbia avuto accesso remoto al sistema. Per questo motivo è impossibile garantire l'integrità di un sistema che è stato vittima di Nimda. L'utente remoto potrebbe aver effettuato delle modifiche nel sistema come:
- Cancellare o modificare le password dei file e degli account;
- Installare dei software che permettono l'attivazione di connessioni remote, conosciuti anche come backdoor;
- Installare dei software di keylogging che permettono di registrare il testo immesso tramite la tastiera;
- Modificare la configurazione di antivirus e firewall in modo da renderli inefficaci;
- Copiare o modificare numeri di carte di credito, informazioni bancarie o personali presenti nel sistema;
- Cancellare o modificare i file e il loro contenuto;
- Inviare materiale incriminante e inappropriato dall'account email della vittima;
- Cancellare informazioni dai file log per nascondere la loro attività

Se si vuole essere certi di stare al sicuro bisogna reinstallare il sistema operativo e riprendere i file personali da un backup eseguito prima di ricevere l'infezione e cambiare tutte le password che erano sul computer infetto e che potrebbero essere state copiate da un intruso.

Raccomandazioni

Per prevenire l'infezione è consigliabile rimuovere o disattivare i servizi non necessari che sfruttano una connessione internet. Come impostazione predefinita, molti sistemi operativi installano dei servizi che non sono fondamentali come per esempio server FTP, telnet e Web server. Questi servizi sono soggetti ad attacchi, ma se sono rimossi c'è minore possibilità di essere infettati e non c'è bisogno di installare tante patch per stare al sicuro. Se avete proprio bisogno di uno di questi servizi, è buona norma assicurarsi di avere tutte le patch aggiornate per evitare che il worm sfrutti uno dei bug ancora presenti. Come al solito, conviene anche utilizzare password complesse (combinazioni casuali di numeri e lettere). Ciò contribuisce a prevenire o limitare danni quando un computer viene infettato. Configurate il vostro server di posta in arrivo per bloccare o rimuovere email che contengono allegati che sono utilizzati comunemente per diffondere i virus, come quelli con estensioni . vbs, . bat, . exe, . pif e . scr. Se un computer è stato già infettato da Nimda, è consigliabile isolarlo rapidamente per evitare ulteriori infezioni su altre macchine. Non aprite gli allegati a meno che non si sia sicuri della loro provenienza e non eseguite i software scaricati da Internet senza aver controllato la presenza di un'infezione. Visitare semplicemente un sito Web infetto può causare l'infezione se determinate vulnerabilità di browser non sono state rattoppate.

{RoSwEIL}